Abstract Algebra

Notes during my Abstract Algebra Course

Zeroeth Edition

Abstract Algebra

Sriaditya Vedantam
svedantam@zyphensvc.com

Contents

This page is intentionally left blank.

Part I

Abstract Algebra

Chapter 1

Introduction to Algebra

The content in this chapter is things to know by heart. We will not be going back and explaining the content discussed in this chapter.

1.1 Logic

For those coming from a pure symbolic proofs-based class, this text will definitely be a bit striking, as I do not like using symbols every time they can be used. It is easier to convey thoughts by just using words and to depict very slight meanings that may not be robotic. It is definitely not impossible to do the mental conversion into symbolic language. However, the way I learned proofs was to use more words than symbols. As a matter of fact, some classes may even deduct points for the overuse of symbols, and I have heard this tale through and through from many people. So take what you will, but I hope this will create some change. If there is one thing to take away from this section, it is that there is nothing ever wrong with using words over symbols, while there is the vice versa.

Let P and Q be statements. It should have been discussed in a proof class the difference between statements, questions, and commands.

[1.1.0.1] Definition (*Basic Logical Statements*). "P **and** Q" This is true if and only if P and Q are both true. This is denoted by $\wedge$.

"P **or** Q" This is true in all cases where at least one of P or Q is true, and false only when they are both false. This is denoted by $\vee$.

"P **implies** Q" We use implications to show that if P holds, then Q follows. For example, we usually write this in English as "If P, then Q." This means that if P is true, then Q will also happen. This is true in $3/4$ of the possible outcomes. Namely, it is true when both P and Q are true, when both are false, and when P is false but Q is true. It is false only when P is true and Q is false. A false premise always makes the implication true. Implications are denoted

by $\implies$.

"P **if and only if** Q" This is called a biconditional, or an equivalence statement. This is short for saying "P implies Q and Q implies P." This is denoted by $\iff$.

"It is not the case that P**"** This is true if and only if P is false. This is also called negation.

1.2 Sets and Classes

Set theory is very much its own field, so we will not be getting into the specifics and the nitty-gritty of each topic. It will just be a brief overview.

[1.2.0.1] Definition (*Sets and Basic Set-Theoretic Language*). **Elements** are either a part of a set or not part of a set. There are infinitely many elements, and they have a choice of being a member of a set. When an element x is a member of a set A, we denote this by

$$x \in A.$$

Otherwise, we say

$$x \notin A.$$

We can also write this out in words as "x is (not) an element of A." These are some of the few things most people use symbols for regardless of their preferences for symbolic language. The following are predicates.

1. "For all" This is denoted by $\forall$.

2. "There exists" This is denoted by $\exists$. The **axiom of extensionality** states that given sets A and B, if for all elements x we have

$$x \in A \iff x \in B.$$

Then $A = B$. If for all elements x, whenever $x \in A$ we also have $x \in B$, then A is a **subset** of B, denoted by $A \subseteq B$.

The **empty set** is a set with no elements, denoted by $\varnothing$.

A **class of sets** is a collection that contains sets and only sets.

The **power axiom** states that for every set A, the power class $P(A)$ contains all subsets of A within a set. This is often denoted by 2^A and has $2^{|A|}$ elements.

A **union of sets** considers all the elements in both sets, denoted by $A \cup B$.

An **intersection of sets** considers only the common elements in both sets, denoted by $A \cap B$.

A **disjoint set** situation occurs when $A \cap B = \varnothing$.

A **family of sets** is a class of sets where each element, mind you a set, is indexed. This is generally denoted by

$$\bigcup_{i \in I} A_i := \{x : x \in A_i \text{ for some } i \in I\}.$$

Similarly, we define

$$\bigcap_{i \in I} A_i.$$

The **complement** of A is related to the negation of A, where we use DeMorgan's Laws.

1.3 Functions

[1.3.0.1] Definition (*Functions and Mappings*). Given sets A and B, a **function** maps f from A to B, denoted by

$$f : A \to B.$$

This means that it assigns each element $a \in A$ to exactly one element $b \in B$. The image of a is written as $f(a) = b$. **Images** refer to the outputs of the function, i.e., the values in B that are hit by elements of A. The **domain** of f is written as f, while B is the **co-domain**, sometimes also referred to as the range. Two functions are equal if they have the same domain, co-domain, and agree on every element of the domain. Suppose $S \subseteq A$. Then the function from S to B defined by

$$g : S \to B \iff g(a) := f(a) \text{ for } a \in S$$

is called the **restriction** of f to S. Let $f : A \to B$ and $g : B \to C$. Then the composite function

$$h : A \to C, \quad h(a) := g(f(a)).$$

Which is called the **composition** of f and g. A function is **injective**, or one-to-one, if for all $a, b \in A$,

$$a \neq b \implies f(a) \neq f(b).$$

This means distinct elements in the domain map to distinct elements in the co-domain. A function is **surjective**, or onto, if for all $b \in B$, there exists $a \in A$ such that

$$f(a) = b.$$

This means every element in the co-domain is hit by at least one element of the domain. A function is **bijective**, or a one-to-one correspondence, if it is both injective and surjective. Given $f : A \to B$ and $g : B \to C$, if f and g are injective, then $g \circ f$ is injective. If $g \circ f$ is injective, then f is injective. If f and g are surjective, then $g \circ f$ is surjective. If $g \circ f$ is surjective, then g is surjective.

1.4 Relations

[1.4.0.1] Definition (*Relations and Cartesian Products*). A **cartesian product** of sets A and B gives us

$$A \times B := \{(a, b) : a \in A,\ b \in B\}.$$

Note that

$$A \times \varnothing = \varnothing = \varnothing \times B.$$

An equivalence relation, denoted by $\sim$, on a set A is a relation satisfying the following properties:

- **reflexive:** $a \sim a$ for all $a \in A$;
- **symmetric:** if $a \sim b$, then $b \sim a$ for all $a, b \in A$;
- **transitive:** if $a \sim b$ and $b \sim c$, then $a \sim c$ for all $a, b, c \in A$.

1.5 Well Ordering and Induction

[1.5.0.1] Definition (*Well-Ordering*). Every nonempty subset of $\mathbb{Z}^{\geq 0}$ contains a smallest element.

This takes into account that there is an order relation ($<$) on all integers of $\mathbb{Z}$. The direct consequence of this definition is mathematical induction. Mathematical induction is a proof technique that uses recursive techniques to prove that a statement is true for all elements past its base case.

[1.5.0.2] Theorem. Assume that $n \in \mathbb{Z}^{\geq 0}$ and $P(n)$ is given.

1. $P(0)$ is a true statement.
2. When $P(k)$ is true, then $P(k+1)$ is also true.

Then $P(n)$ is true for all $n \in \mathbb{Z}^{\geq 0}$.

$\therefore$

Proof. A remark on this theorem is that $P(k)$ does not have to be true, but we assume so. This is called the induction hypothesis.

In proof writing, if we are given an "If... Then..." statement, we generally assume that the statement before the "Then" is true, and attempt to prove the rest. This is the same thing we have proved through induction. It can be seen as a result of continued direct proofs compiled

together and generalized to become the induction we know today.

The following example is how we use induction in today's world, and it is important to note how we use it compared to how one may have done it for a proofs course. In other words, this is a practical application of how a researcher would use induction. □

[1.5.0.3] EXAMPLE. A set of n elements has 2^n subsets.

$P(0)$: $2^0 = 1$ subset.

$P(1)$: $2^1 = 2$ subsets.

$P(3)$: $2^3 = 8$ subsets.

Assume $P(k)$, namely that a set with k elements has 2^k subsets. Now prove that $P(k+1)$ says a set with $k+1$ elements has 2^{k+1} subsets. In a more standardized proof writing, we can define a set

$$S := \{n \in \mathbb{Z}^{\geq 0} : P(n) \text{ is true}\},$$

and show that $S = \mathbb{Z}^{\geq 0}$. Let our induction hypothesis be "$P(k)$ is true." Since we have shown that our base case $P(0)$ is true, we assume $P(k)$ is true and attempt to prove $P(k+1)$. Suppose a set has k elements. If we add one new element, then every old subset has exactly two choices: either include the new element or do not include it. Therefore the number of subsets doubles. Hence the new set has

$$2 \cdot 2^k = 2^{k+1}$$

subsets. Thus $P(k+1)$ is true. Therefore, by induction, $P(n)$ is true for all $n \in \mathbb{Z}^{\geq 0}$.

1.6 A variation on Induction

Now with mathematical induction, also just referenced as induction, we can also show another type called strong or complete induction.

[1.6.0.1] THEOREM. Assume that $n \in \mathbb{Z}^{\geq 0}$ and $P(n)$ is given. If

1. $P(0)$ is true, and
2. for all $t \in \mathbb{Z}^{\geq 0}$, if $P(j)$ is true for all j such that $0 \leq j \leq t$, then $P(t+1)$ is also true,

then $P(n)$ is true for all $n \in \mathbb{Z}^{\geq 0}$.

$\therefore$

Proof. Let us prove this using ordinary induction. Let our induction hypothesis be that $P(j)$ is true for all j such that $0 \leq j \leq t$. Define the set

$$S := \{n \in \mathbb{Z}^{\geq 0} : P(j) \text{ is true for all } j \text{ such that } 0 \leq j \leq n\}.$$

For the base case, let $n = 0$. Then $P(0)$ is true, so $0 \in S$. Now suppose $k \in S$. Then $P(j)$ is true for all j such that $0 \leq j \leq k$. By the hypothesis, this implies $P(k+1)$ is true. Hence $k+1 \in S$. Therefore, by induction, $S = \mathbb{Z}^{\geq 0}$. Thus $P(n)$ is true for all $n \in \mathbb{Z}^{\geq 0}$. □

Similar to how we used weak or regular induction to prove complete induction, we can do the same in reverse. In fact, we can prove all of these theorems and definitions using one another. We can use the well-ordering axiom to prove mathematical induction and use mathematical induction to prove complete induction. To complete the loop, we can prove well-ordering through complete induction. On a harder note, we can prove regular induction through complete induction, but it is possible.

[1.6.0.2] Theorem. Well-Ordering implies Induction.

$$\therefore$$

Proof. Let us define the set

$$S := \{n \in \mathbb{Z}^{\geq 0} : P(n) \text{ is false}\} \subseteq \mathbb{Z}^{\geq 0}.$$

Our goal is to show that $S = \varnothing$. Assume $S \neq \varnothing$. Then by well-ordering, let $d \in S$ be the smallest element. Since $P(0)$ is true, we must have $d \neq 0$. Hence $d \geq 1$, so $d - 1 \in \mathbb{Z}^{\geq 0}$. Since d is the smallest element of S, we must have $d-1 \notin S$. Thus $P(d-1)$ is true. By the induction hypothesis, $P(d-1) \implies P(d)$. Hence $P(d)$ is true, which contradicts the fact that $d \in S$. Therefore $S = \varnothing$. Hence $P(n)$ is true for all $n \in \mathbb{Z}^{\geq 0}$. □

Now that we have jump-started the proof writing structure in our heads, let us go ahead and start this course with our next topic: Fundamentals of Arithmetic and Divisibility.

Chapter 2

Fundamentals of Arithmetic and Divisibility

2.1 Axioms

Axioms are trivial definitions used in everyday life, or even mathematics, that we take for granted. They are definitions that are inarguable and are the core of mathematics today.

I never quite understood the hierarchy of math statements, but this is a way to look at it. Axioms are a specific type of definition that is just taken as a fact or true. Definitions are similar to axioms in that they build the premise of future statements, and these may or may not include proofs to explain why they are true. Lemmas are true statements that are not important in the long run, but are useful for understanding future statements, and are generally associated with proofs. Propositions are important statements that must be associated with proofs and are vital building blocks in research. Theorems are big conclusions that wrap each concept mentioned in a paper into one central idea and are even more important than propositions, and these also require proofs to be stated alongside the statement.

Now the following axioms or properties are what we accept without another thought, but they are important to mention to understand future content when they are brought up again.

[2.1.0.1] Definition (*Additive Properties*).

1. Addition is well-defined. Given $a, b \in \mathbb{Z}$, $a + b$ is a uniquely defined integer.
2. Substitution Law. Since addition is well-defined, if $a = b$ and $c = d$, then $a + c = b + d$.
3. Commutative Law. For all $a, b \in \mathbb{Z}$, $a + b = b + a$.
4. Associative Law. For all $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$.
5. There exists a zero element $0 \in \mathbb{Z}$, called the additive identity, satisfying $0 + a = a$ for any $a \in \mathbb{Z}$.

6. For all $a \in \mathbb{Z}$, there exists a unique additive inverse $-a \in \mathbb{Z}$ satisfying $a + (-a) = 0$.

[2.1.0.2] Definition (*Multiplicative Properties*).

1. Multiplication is well-defined. Given $a, b \in \mathbb{Z}$, $a \cdot b$ is a uniquely defined integer.
2. Substitution Law. If $a = b$ and $c = d$, then $ac = bd$.
3. $\mathbb{Z}$ is closed under multiplication. For all $a, b \in \mathbb{Z}$, $a \cdot b \in \mathbb{Z}$.
4. Commutative Law. For all $a, b \in \mathbb{Z}$, $ab = ba$.
5. Associative Law. For all $a, b, c \in \mathbb{Z}$, $(ab)c = a(bc)$.
6. There exists a multiplicative identity $1 \in \mathbb{Z}$ satisfying $1 \cdot a = a$ for all $a \in \mathbb{Z}$.

[2.1.0.3] Definition (*Distributive Property*). For all $a, b, c \in \mathbb{Z}$,

$$a(b + c) = ab + ac.$$

[2.1.0.4] Definition (*Trichotomy Principle*). $\mathbb{Z}$ can be split into three distinct sets:

$$\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}.$$

[2.1.0.5] Definition (*Positivity Axiom*). The sum or product of positive integers is positive.

[2.1.0.6] Definition (*Discrete Property*). We have learned these already, namely the Well-Ordering Principle of $\mathbb{N}$ and the Principle of Induction.

2.2 Division

Now that we have learned the axioms of arithmetic, let us learn about the division algorithm.

We have all, hopefully, learned how to divide in grade school. As a revision, you can divide a number evenly by some other number and whatever is left over will result as the remainder. This can be written more formally as

$$\text{dividend} = (\text{divisor})(\text{quotient}) + (\text{remainder}).$$

Now there is an important understanding I wanted to show to the audience. Every basic arithmetic operation can be written in terms of addition and multiplication. We will later see with rings that

we make our lives easier by doing subtraction, which shows both an inverse and additive property. But for now, that is all mumbo-jumbo.

[2.2.0.1] THEOREM (*Division Algorithm*). Suppose $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist $q, r \in \mathbb{Z}$ such that

$$a = qb + r$$

with

$$0 \leq r < b.$$

$$\therefore$$

Proof. Let there be a set S such that

$$S := \{a - xb : a - xb \geq 0,\ x \in \mathbb{Z}\}.$$

We first check that $S \neq \varnothing$. Given a and b, find x such that $a - xb \geq 0$. If $a \geq 0$, let $x = 0$. Then $a - xb = a \geq 0$. If $a < 0$, let $x = a$. Then

$$a - ab = a(1 - b),$$

and since $b > 0$, we have $b \geq 1$, therefore $1 - b \leq 0$. Since $a < 0$ as well, it follows that $a(1-b) \geq 0$. Since $S \neq \varnothing$, then S is well-ordered. Thus there exists $r \in S$ such that r is the smallest element of S. Claim: $r \geq 0$ and $r < b$. Since $r \in S$, there exists $q \in \mathbb{Z}$ such that $r = a - qb$ and $r \geq 0$. It remains to prove that $r < b$. Suppose $r \geq b$. Then let

$$\begin{aligned} d &= a - (q+1)b \\ &= a - qb - b \\ &= r - b. \end{aligned}$$

Since $r \geq b$, we have $r - b \geq 0$. Thus $d \in S$. But $d = r - b < r$, which contradicts the fact that r is the smallest element of S. Therefore $r < b$. Hence

$$a = qb + r$$

with $0 \leq r < b$. □

There is a lot to dissect here. I want to dedicate special focus to this theorem. This will lay the foundation, so glance your eyes on this beauty and take it in its glory. But in all seriousness, this is a really important topic to take in, so let us explain it thoroughly. Similar to what we have in Figure 2.1 with the dividend equation, we just broke it down and generalized it using proof notation. So given that a is some dividend, we have divisor b, and quotient q that are multiplied, then added with remainder r. There is also a reason why the division algorithm requires that r be less than b but at minimum 0. This may be trivial, but if r is greater than b, we can subtract b from r and get a new remainder. It has the most optimized equation. Now that we understand what we are doing in more understandable terms, let us look at our proof itself and implement it as a core memory as how a child may remember their guardian.

[2.2.0.2] EXAMPLE. Let S be a set of remainders. We can do this through example. If

$$a = 81,$$

$$b = 8,$$

and x is a variable, then

$$r = a - bx.$$

If we let $x = 1$, then $r = 73$.

If we let $x = 4$, then $r = 49$.

If we let $x = 10$, then $r = 1$.

If we let $x = 11$, then $r = -7$.

However, r can only be at minimum 0, therefore r cannot be -7. Therefore our most optimized r is when $x = 10$. Of course, x can go in the opposite direction, since we did not bound $\mathbb{Z}$ only to non-negative integers.

Thus we have shown an example of the division algorithm. Now that we understand the values that set S can contain, even though we have provided proof, we must still prove this through math and generalize it. And that is exactly what we spend the rest of the proof doing.

We answer questions in this proof such as, what if a is greater than 0 or less than 0. And what happens if r is greater than b, which we show cannot happen if r is the smallest non-negative integer of that form. For example, we could technically have a solution

$$a = 200,$$
$$b = 2,$$
$$x = 10,$$
$$r = 180,$$

and this fits the equation $a = bx + r$, but it is not the division algorithm remainder because r is not the smallest allowable one.

[2.2.0.3] Proposition (*Uniqueness in the Division Algorithm*). The integers $q, r \in \mathbb{Z}$ in the division algorithm are unique.

$\therefore$

Proof. Given $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ with $b > 0$, suppose

$$a = q_1 b + r_1$$

such that $q_1, r_1 \in \mathbb{Z}$ and $0 \leq r_1 < b$. Also suppose that

$$a = q_2 b + r_2$$

such that $q_2, r_2 \in \mathbb{Z}$ and $0 \leq r_2 < b$. Claim: $q_1 = q_2$ and $r_1 = r_2$. We have

$$a = q_1 b + r_1$$

$$a = q_2 b + r_2.$$

Subtracting gives

$$0 = (q_1 - q_2)b + r_1 - r_2$$
$$r_2 - r_1 = (q_1 - q_2)b.$$

Since $0 \leq r_1, r_2 < b$, we have

$$-b < r_2 - r_1 < b.$$

Therefore

$$-b < (q_1 - q_2)b < b.$$

Since $b > 0$, dividing through by b yields

$$-1 < q_1 - q_2 < 1.$$

Since $q_1 - q_2 \in \mathbb{Z}$, the only possibility is

$$q_1 - q_2 = 0.$$

Therefore $q_1 = q_2$. Then

$$0 = (q_1 - q_2)b + r_1 - r_2$$
$$0 = (0)b + r_1 - r_2$$
$$0 = r_1 - r_2.$$

Thus $r_1 = r_2$. □

This proposition demonstrates that q and r are unique, and this is really important to show in math when we are proving an algorithm. Regardless of what q and r are, if they exist, then they are unique, sounding trivial, but as we see the proof is rather less trivial.

This one is a bit more straightforward, therefore there will not be a conceptualizing analysis on this proof. This is also just further building the proof techniques we have at our arsenal and allowing one to understand the algorithm through and through.

[2.2.0.4] Definition (*Logical Divide*). Suppose $a, b \in \mathbb{Z}$. Let us define the logical divide of b divides a as $b \mid a$. If there exists $q \in \mathbb{Z}$ such that

$$a = bq,$$

then $b \mid a$. If $b = 0$ and $a \neq 0$, then $b \nmid a$, because $0q = 0$, and $a \neq 0$.

There is not a strict name for this definition as far as I know, therefore I created a name for it, Logical Divide. It is the logical notation for the phrase "x divides y", and it is trivial to Abstract Algebra.

It is slightly different from, say, previous computationally algebraic courses, where one just computes some division and may even end up with a completed or incomplete, rational or not, answer. Note that up to now we are only sticking with the integers, and this is a really important fact to keep in mind. Therefore when we say that $2 \mid 4$, then we really mean that 4 is evenly divisible by 2, but 3 does not divide 4, even if we can write it in terms of a decimal.

Another way we can explain this topic is through the division algorithm. If it does not look similar, we can write b divides a as

$$a = bq + r,$$

where $r = 0$. Now does this mean that if $a = 0$, then does $0 \mid 0$. Honestly, it is a debated topic in algebra and number theory. Some may state yes, others may state no. But what is important is that many people leave it undefined, for the same reason why your calculator cannot divide 0 by 0. Now if $a = 0$ and $b \mid a$, there is an integer q in $\mathbb{Z}$ such that $a = bq$. This is a proof we will not get into for the sake of saving time and space, but it is a nice practice exercise. One proof we will be looking at is the following.

[2.2.0.5] Lemma. Assume $b \mid a$ and $b \neq 0$, so $a = bq$ for some $q \in \mathbb{Z}$. Then $-b \mid a$.

$\therefore$

Proof. We have

$$a = (-b)(-q),$$

so $-b \mid a$, since $-q \in \mathbb{Z}$. Similarly, $b \mid -a$. □

This is just a fun fact to rationalize that these four results are possible: $b \mid a$, $b \mid -a$, $-b \mid a$, and $-b \mid -a$. Now on a larger note, we must prove transitivity through logical divides.

[2.2.0.6] Lemma. Suppose $a, b, c \in \mathbb{Z}$. If $c \mid b$ and $b \mid a$, then $c \mid a$.

$\therefore$

Proof. There exist $q_1, q_2 \in \mathbb{Z}$ such that

$$a = bq_1$$

and

$$b = cq_2.$$

So

$$a = (cq_2)q_1 = c(q_2q_1).$$

Since $q_2q_1 \in \mathbb{Z}$, we have $c \mid a$. □

One thing to note is that divisibility is not symmetric, which means that if $b \mid a$, it does not follow that $a \mid b$ unless we are in a special case such as $a = \pm b$. There is a statement that could be said about linear combinations of a and b. If there is an integer c that divides both a and b, then for any integers x and y, we have

$$c \mid xa + yb.$$

Therefore, c divides any linear combination of a and b. The proof of this is similar to the previous proof before. The idea is that if you can write a and b in terms of c, then the linear combination can also be written in terms of c. Thus showing divisibility. Try to implement this on your own. If it has not been noticeable, there is nothing more to learning a course outside of learning the definitions and theorems.

[2.2.0.7] Definition (*Greatest Common Divisor*). The GCD of a and b, written as $\gcd(a,b) = d$, is the integer $d > 0$ such that $d \mid a$ and $d \mid b$, and if $c \mid a$ and $c \mid b$, then $c \mid d$.

The greatest common divisor is a concept that we have learned in grade school. If we recall, we can write $\gcd(4,6) = 2$, since $2 \mid 4$ and $2 \mid 6$.

[2.2.0.8] Theorem (*Linear Combinations of GCD*). Let $a, b \in \mathbb{Z}$, not both 0. Let there be a set S such that

$$S := \{xa + yb : x, y \in \mathbb{Z},\ xa + yb > 0\}.$$

Then $S \neq \varnothing$, and by the Well-Ordering Principle, S has a smallest element called d. Then $d = \gcd(a,b)$. The key statement is that if $d = \gcd(a,b)$, then there exist $x, y \in \mathbb{Z}$ such that

$$d = xa + yb.$$

$\therefore$

Proof. Let $S \neq \varnothing$. Then there exists $d \in S$ such that for all $t \in S$, we have $d \leq t$. Since $d \in S$, there exist $x, y \in \mathbb{Z}$ such that

$$d = xa + yb.$$

Now our goal is to prove that $d \mid a$. Since $d > 0$, by the Division Algorithm there exist $q, r \in \mathbb{Z}$ such that

$$a = qd + r$$

with

$$0 \leq r < d.$$

Suppose $r > 0$. Then

$$\begin{aligned} r &= a - qd \\ &= a - q(xa + yb) \\ &= a - qxa - qyb \\ &= (1 - qx)a - (qy)b. \end{aligned}$$

So r is a linear combination of a and b. Since $r > 0$ and $r < d$, then $r \in S$, contradicting the assumption that d is the smallest element of S. Therefore $r = 0$. Hence $a = qd$, so $d \mid a$. Similarly, we can show $d \mid b$. Now suppose $c \mid a$ and $c \mid b$. Then $c \mid xa + yb$, which is a linear combination of a and b, and this equals d. Therefore $c \mid d$. Hence $d = \gcd(a,b)$. □

If the gcd of any two integers ever equals 1, then we say that a and b are relatively prime. If they are relatively prime, then by the previous theorem, the linear combination will also equal 1.

[2.2.0.9] Theorem. Suppose $\gcd(a,b) = 1$ and $c \in \mathbb{Z}$ such that $a \mid bc$. Then $a \mid c$.

$\therefore$

Proof. Since $\gcd(a,b) = 1$, there exist $x, y \in \mathbb{Z}$ such that

$$xa + yb = 1.$$

Therefore,

$$xa + yb = 1$$
$$cxa + cyb = c$$
$$(cx)a + y(bc) = c.$$

Now $a \mid (cx)a$ and by assumption $a \mid bc$, so $a \mid y(bc)$ as well. Therefore $a \mid c$. □

The last thing we will be looking at in this section is the extended gcd algorithm. The idea behind this is to use the gcd algorithm and then reverse the process in order to find the factors of the linear combination. This is more of a computational math.

The gcd algorithm can be written in terms of the Division Algorithm and continuing to find the terms that make up the two factors. An idea of this is using $\gcd(109, 26)$.

$$109 = 26(4) + 5.$$

Because 109 can be split up by 26 and have a remainder of 5, this is no different from having a gcd of $(26, 5)$.

$$26 = 5(5) + 1.$$

Now because we are left with a remainder of one, and one can go into any number, then 1 is our final answer for the gcd of $(109, 26)$. This is a way to do the gcd algorithm through division.

But what if we are to set this the other way around.

$$1 = 26 - 5(5).$$

Similar to what we did before, we are shifting all elements in the equation to create the one above.

$$1 = 26 - 5(109 - 26(4)).$$
$$1 = (-5)(109) + (21)(26).$$

Thus we have found the linear combination factors of the equation.

2.3 Primes

I am excited about this topic because it practically is my field of interest.

[2.3.0.1] Definition (*Prime Integer*). Let $p \in \mathbb{Z}$. We say that p is prime if the only divisors of p are $-1, 1, -p, p$, and

$$p \neq -1, 0, 1.$$

This definition has two criteria. First, the divisors of p are restricted. Second, p is not equal to certain restricted values. We use the term restricted to denote more so a finite set of values, though that sounds like a stronger claim. By the only divisors of p, we mean that if you divide p by any other integer, using the division algorithm, we will get a remainder. Using the previous content learned, we will see that the gcd of p and any integer relatively prime to it is 1. When we have p not equal to a select few values, then this ensures that the prime number does not contradict the first criterion. This definition helps identify and distinguish prime numbers from other integers.

[2.3.0.2] Theorem (*Euclid's Lemma*). Suppose p is prime, and let $b, c \in \mathbb{Z}$. If

$$p \mid bc,$$

then

$$p \mid b \quad \text{or} \quad p \mid c.$$

$\therefore$

Proof. Suppose $p \nmid b$. We claim that

$$\gcd(p, b) = 1.$$

Let $d = \gcd(p, b)$. Then $d > 0$, $d \mid p$, and $d \mid b$. Since p is prime, the only positive divisors of p are 1 and $|p|$. Thus $d = 1$ or $d = |p|$. But $d \neq |p|$, because if $|p| \mid b$, then in particular $p \mid b$, contradicting our assumption. Therefore

$$\gcd(p, b) = 1.$$

By the previous theorem on relatively prime integers, since $\gcd(p, b) = 1$ and $p \mid bc$, it follows that

$$p \mid c.$$

Hence if $p \mid bc$, then either $p \mid b$ or $p \mid c$. □

This "lemma" is something Euclid used to prove something bigger. The name stuck as "Euclid's Lemma", however, it is the foundation for fields such as Number Theory. Its more appropriate name is the Fundamental Property of Prime Numbers. It sounds like a really basic lemma, but it undermines its true essence. It shows that prime numbers are the building blocks of all integers and that a number divisible by a prime must be divisible by that prime individually or by another prime factor.

[2.3.0.3] Theorem (*Fundamental Theorem of Arithmetic (FTA)*). If $n \in \mathbb{Z}$ and

$$n \neq -1, 0, 1,$$

then n can be written uniquely as a product of primes, up to order and sign.

$\therefore$

Proof. We will prove this after one useful lemma. □

[2.3.0.4] Lemma. Suppose p is prime, and let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ such that

$$p \mid a_1 a_2 \cdots a_n.$$

Then

$$p \mid a_i$$

for some $i \in \{1, \ldots, n\}$.

∴

Proof. We prove this by induction on n. If $n = 1$, then the statement is immediate. If $n = 2$, then this is exactly Euclid's Lemma. Now suppose the statement is true for $n = k$. Assume

$$p \mid a_1 a_2 \cdots a_k a_{k+1}.$$

Then

$$p \mid (a_1 a_2 \cdots a_k) a_{k+1}.$$

By Euclid's Lemma,

$$p \mid a_1 a_2 \cdots a_k$$

or

$$p \mid a_{k+1}.$$

If $p \mid a_{k+1}$, then we are done. If $p \mid a_1 a_2 \cdots a_k$, then by the induction hypothesis,

$$p \mid a_i$$

for some i with $1 \leq i \leq k$. Therefore

$$p \mid a_i$$

for some $i \in \{1, \ldots, k+1\}$. □

[2.3.0.5] Theorem (*Proof of the Fundamental Theorem of Arithmetic*). If $n \in \mathbb{Z}$ and

$$n \neq -1, 0, 1,$$

then n can be written uniquely as a product of primes, up to order and sign.

∴

Proof. Claim 1. Existence of factorization. Suppose $n \in \mathbb{Z}$ and $n \neq -1, 0, 1$. We first show that n can be written as a product of primes. If $n < 0$, then $n = -m$ for some positive integer m. So once we prove the result for positive integers greater than 1, the negative case follows by attaching a minus sign. Now use strong induction on $n \in \mathbb{N}$ with $n \geq 2$. If n is prime, then we are done. If n is not prime, then there exist integers a, b such that

$$n = ab$$

with

$$1 < a < n \quad \text{and} \quad 1 < b < n.$$

By the induction hypothesis, both a and b can be written as products of primes. Hence n can also be written as a product of primes. So existence is proved.

Claim 2. Uniqueness of factorization. Suppose

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

where all p_i and q_j are prime. We prove uniqueness by induction on $\min\{r, s\}$. If $\min\{r, s\} = 1$, then we may assume $r = 1$. So

$$p_1 = q_1 q_2 \cdots q_s.$$

Since p_1 is prime and divides the product on the right, by the previous lemma,

$$p_1 \mid q_j$$

for some j. Because q_j is prime, this implies

$$q_j = \pm p_1.$$

Since both sides factor n, this forces $s = 1$, and the factorizations agree up to sign. Now assume uniqueness holds whenever the minimum number of prime factors is k. Suppose

$$p_1 p_2 \cdots p_{k+1} = q_1 q_2 \cdots q_s$$

with $\min\{k+1, s\} = k+1$. Since p_1 divides the right-hand side, by the lemma,

$$p_1 \mid q_j$$

for some j. Because q_j is prime, we have

$$q_j = \pm p_1.$$

After rearranging, we may assume

$$q_1 = \pm p_1.$$

Canceling this common prime factor up to sign leaves

$$p_2 \cdots p_{k+1} = \pm q_2 \cdots q_s.$$

Now the minimum number of prime factors has dropped to k, so by the induction hypothesis, the remaining primes agree up to order and sign. Therefore the original factorization is unique up to order and sign. □

Chapter 3

Congruence Classes in $\mathbb{Z}$

3.1 Congruences

When we talk about congruence classes mod n, we are essentially grouping integers based on the remainder they leave when divided by n. This creates a classification system, where numbers that share the same remainder form a class.

[3.1.0.1] Definition (*Congruence*). Suppose $n \in \mathbb{N}$. If $a, b \in \mathbb{Z}$, we define

$$a \equiv b \mod n$$

as a congruence. We say "a is congruent to b modulo n" if and only if

$$n \mid (b - a).$$

[3.1.0.2] Lemma. $a \equiv b \mod n$ if and only if $n \mid a - b$, and this holds if and only if there exists $q \in \mathbb{Z}$ such that

$$b = qn + a.$$

Prove this exercise on your own.

$\therefore$

Proof. □

[3.1.0.3] Definition (*Equivalence Relation*). Given S is a set and $\sim$ is a relation on S, $\sim$ is an equivalence relation if for all $a, b, c \in S$,

1. $a \sim a$ (reflexive);
2. if $a \sim b$, then $b \sim a$ (symmetric);
3. if $a \sim b$ and $b \sim c$, then $a \sim c$ (transitive).

We will learn and find uses for the equivalence relation, but to connect it to the topics at hand, $a \equiv b \mod n$ is an equivalence relation that envelopes congruences and what we will learn about congruence classes. Essentially, $a \equiv b \mod n$ is the same as $a \sim b$.

[3.1.0.4] Lemma. Congruence mod n is an equivalence relation.

$\therefore$

Proof. **Case 1.** Let $a \in \mathbb{Z}$. Then $a \equiv a \mod n$, because $a - a = 0$ and $n \mid 0$.

Case 2. Suppose $a \equiv b \mod n$. Then $n \mid a - b$, and due to properties of the logical divide, $n \mid b - a$. Thus $b \equiv a \mod n$.

Case 3. Suppose $a, b, c \in \mathbb{Z}$, $a \equiv b \mod n$, and $b \equiv c \mod n$. So $n \mid b - a$ and $n \mid c - b$. Then $n \mid (b - a) + (c - b) = c - a$. Thus $a \equiv c \mod n$. □

[3.1.0.5] Definition (*Equivalence Classes*). Suppose $\sim$ is an equivalence relation on S and $a \in S$. The equivalence class of a is

$$[a] := \{b \in S : b \sim a\}.$$

Let us consider an equivalence relation $\sim$ on the set of integers $\mathbb{Z}$, where $a \sim b$ if and only if $a \equiv b \mod 5$. In this case,

$$[2]_5 = \{\ldots, -8, -3, 2, 7, 12, \ldots\}.$$

This is the equivalence class of 2, consisting of all integers that are congruent to 2 modulo 5. Equivalence classes provide a systematic way of grouping elements in a set based on their relationships under an equivalence relation.

[3.1.0.6] Definition (*Congruence Classes*). For a congruence mod n, if $a \in \mathbb{Z}$, then

$$[a] := \{b \in \mathbb{Z} : b \equiv a \mod n\}.$$

Congruence classes provide a systematic way of grouping integers based on their remainders when divided by n under a congruence relation. They are essential in modular arithmetic, number theory, and algebraic structures, contributing to a deeper understanding of mathematical relationships and structures.

Two equivalence classes are the same if they include each other. For example, if $[a] = [b]$, then $a \in [b]$ and $b \in [a]$. The set S is the distinct union of its distinct equivalence classes. That is, every element of S is in some equivalence class.

[3.1.0.7] Proposition. If $a, b \in S$, then either $[a] = [b]$ or $[a] \cap [b] = \varnothing$.

$\therefore$

Proof. We need to prove that if

$$[a] \cap [b] \neq \varnothing,$$

then

$$[a] = [b].$$

Let $c \in [a] \cap [b]$. Then $c \equiv a \mod n$ and $c \equiv b \mod n$. So by the next proposition,

$$[c] = [a] = [b].$$

Thus $[a] = [b]$. □

[3.1.0.8] Proposition. [a] = [b] $\iff a \equiv b \mod n$.

∴

Proof. ($\implies$) By definition,

$$[a] := \{x : x \equiv a \mod n\}.$$

Since $a \equiv a \mod n$, we have $a \in [a]$. If $[a] = [b]$, then $a \in [b]$. But

$$[b] := \{x \in \mathbb{Z} : x \equiv b \mod n\},$$

so $a \equiv b \mod n$.

($\impliedby$)

Case 1. $[a] \subseteq [b]$. Let $c \in [a]$. Then $c \equiv a \mod n$. Since $a \equiv b \mod n$, by transitivity we get $c \equiv b \mod n$. So $c \in [b]$. Hence $[a] \subseteq [b]$. Similarly, we can show $[b] \subseteq [a]$. Thus $[a] = [b]$. □

This relationship provides a clear connection between the equality of equivalence classes and the congruence of integers modulo n.

[3.1.0.9] Proposition. Fix $n \geq 2$. The distinct congruence classes modulo n are

$$[0], [1], \ldots, [n-1].$$

In fact, if $a \in \mathbb{Z}$, then $[a] = [r]$ where r is the remainder when a is divided by n.

∴

Proof. If

$$a = qn + r, \quad 0 \leq r \leq n-1,$$

then $a \equiv r \mod n$, so $[a] = [r]$. By the division algorithm, every integer a has such a remainder r, so every class $[a]$ must be one of these classes. To show these classes are distinct, suppose $[i] = [j]$ where $0 \leq i, j \leq n-1$. Then by the previous proposition,

$$i \equiv j \mod n.$$

So $n \mid (j - i)$. But since $-(n-1) \leq j - i \leq n-1$, the only multiple of n in this range is 0. Thus $j - i = 0$, so $i = j$. Therefore the distinct congruence classes modulo n are exactly

$$[0], [1], \ldots, [n-1].$$

□

3.2 Modular Arithmetic

[3.2.0.1] Definition (*Modular Arithmetic*). Fix $n \in \mathbb{Z}^{\geq 2}$. Define addition and multiplication on congruence classes mod n by

$$[a] + [b] := [a + b]$$

and

$$[a] \cdot [b] := [ab].$$

Given this definition, it seems a little ambiguous if you really sit down and analyze it, but we come to learn that this gives us properties that allow this arithmetic to be well-defined. This definition shows that it is closed under addition and multiplication, and I will leave that up to the reader to figure out how to find such values.

[3.2.0.2] Theorem. If $a, b, c, d \in \mathbb{Z}$ with $a \equiv c \mod n$ and $b \equiv d \mod n$, then

$$a + b \equiv c + d \mod n$$

and

$$ab \equiv cd \mod n.$$

$\therefore$

Proof. Given $n \mid c - a$ and $n \mid d - b$, we have

$$(c + d) - (a + b) = (c - a) + (d - b).$$

Thus $n \mid ((c + d) - (a + b))$, so

$$a + b \equiv c + d \mod n.$$

Also,

$$cd - ab = d(c - a) + a(d - b).$$

Since $n \mid c - a$ and $n \mid d - b$, it follows that

$$n \mid d(c - a) + a(d - b) = cd - ab.$$

Therefore

$$ab \equiv cd \mod n.$$

□

[3.2.0.3] Theorem (*Well-Defined Modular Arithmetic*). Modular arithmetic is well-defined.

$\therefore$

Proof. Suppose $[a] = [c]$ and $[b] = [d]$. Then $a \equiv c \mod n$ and $b \equiv d \mod n$. By the previous theorem,

$$a + b \equiv c + d \mod n$$

and

$$ab \equiv cd \mod n.$$

Thus

$$[a+b] = [c+d]$$

and

$$[ab] = [cd].$$

□

[3.2.0.4] Definition ($\mathbb{Z}_n$). The set of congruence classes mod n is

$$\mathbb{Z}_n := \{[a] : a \in \mathbb{Z}\} = \{[0], [1], \ldots, [n-1]\}.$$

For example, in $\mathbb{Z}_4$, addition is defined by:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Multiplication in $\mathbb{Z}_4$ is defined by:

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Commutative, associative, and distributive hold for $\mathbb{Z}_n$. The additive identity is

$$[0] + [a] = [a].$$

The multiplicative identity is

$$[1][a] = [a].$$

[3.2.0.5] Axiom (*Additive inverses in* $\mathbb{Z}_n$). Every element in $\mathbb{Z}_n$ has an additive inverse.

$$[a] + [-a] = [0].$$

3.3 Units and Divisors

[3.3.0.1] Definition (*Units in Congruence Classes*). $[a]$ is a unit if $[a]$ has a multiplicative inverse. That is, there exists $[x] \in \mathbb{Z}_n$ such that

$$[a][x] = [1].$$

[3.3.0.2] Theorem. $[a]$ is a unit if and only if $\gcd(a, n) = 1$.

$\therefore$

Proof. □

[3.3.0.3] Proposition. All nonzero classes in $\mathbb{Z}_p$ are units.

$\therefore$

Proof. Suppose $[a] \in \mathbb{Z}_p$ with $[a] \neq [0]$. Then $p \nmid a$. Since p is prime, this implies

$$\gcd(a, p) = 1.$$

By Bézout's Identity, there exist integers x, q such that

$$ax + qp = 1.$$

Thus

$$ax \equiv 1 \mod p,$$

so

$$[a][x] = [1].$$

Therefore $[a]$ is a unit. □

Easy to show the converse by showing a multiplicative inverse in $\mathbb{Z}_p$. So $[a]$ has a multiplicative inverse. This proposition, using $n \neq p$, will show it is true for the previous theorem. To test whether $[a]$ is a unit in $\mathbb{Z}_{32}$ and find $[a]^{-1}$ in $\mathbb{Z}_{32}$, let $a = 4$ and try to find an $x \in \mathbb{Z}$ such that

$$4x + 32q = 1.$$

But

$$\gcd(4, 32) = 4 \neq 1,$$

so no such integers x, q exist. Therefore $[4]$ is not a unit in $\mathbb{Z}_{32}$. So there is no inverse to find.

[3.3.0.4] Definition (*Zero-Divisors*). $[a]$ is a zero-divisor in $\mathbb{Z}_n$ if there exists $[x] \neq [0]$ such that

$$[ax] = [0].$$

[3.3.0.5] Theorem. $[a]$ is a zero-divisor in $\mathbb{Z}_n$ if and only if $\gcd(a, n) \neq 1$.

$\therefore$

Proof. Let us prove the contrapositive in one direction. Suppose $\gcd(a,n) = 1$. Then $[a]$ is a unit in $\mathbb{Z}_n$ by the previous theorem. We will show that $[a]$ is not a zero-divisor. Suppose $[ab] = [0]$ for some $b \in \mathbb{Z}$. Since $[a]$ is a unit, there exists $[x] \in \mathbb{Z}_n$ such that

$$[xa] = [1].$$

Then

$$[x]([ab]) = [x][0] = [0],$$

so

$$[xa][b] = [1][b] = [b] = [0].$$

Thus $[ab] = [0]$ implies $[b] = [0]$. Therefore $[a]$ is not a zero-divisor. Conversely, suppose $\gcd(a,n) = d > 1$. Write

$$a = da_1, \qquad n = dn_1.$$

Then

$$an_1 = da_1n_1 = a_1n,$$

so

$$[a][n_1] = [0].$$

Also, since $d > 1$, we have $0 < n_1 < n$, hence

$$[n_1] \neq [0].$$

Therefore $[a]$ is a zero-divisor in $\mathbb{Z}_n$. □

For example, if we take $\mathbb{Z}_{12}$, then since

$$\gcd(4,12) = 4,$$

$[4]$ is a zero-divisor.

Chapter 4

Rings

Around this chapter is where most textbooks will start. Some of the concepts that we introduced in the previous chapters are more seen as prior knowledge, or seen in an introduction chapter similar to what we have with Chapter 1. So from here on out, consider everything you learned so far as a foundation for the rest of the content.

4.1 Rings

[4.1.0.1] Definition (*Ring*). A ring R is a set with two operations, $+$ and $\times$. Addition is commutative and associative. There exists an additive identity, usually denoted by 0_R. There exists an additive inverse in R, say b, such that $a+b=0_R$, and this inverse is unique. Multiplication is associative. Together, the two operations satisfy the distributive laws. There may also be a multiplicative identity, denoted by 1_R.

[4.1.0.2] Definition (*Subrings*). A subset S is a subring of R if for all $a,b\in S$, it has closure under addition and multiplication. It must also have the additive identity and additive inverses for each element.

For example, in an introduction to proofs class we may have seen that

$$\mathbb{Z}\subseteq\mathbb{Q}\subseteq\mathbb{R}\subseteq\mathbb{C}.$$

We learned them as sets, but looking at properties of rings and subrings, consider them all rings and subrings in that order. However, if we wanted to look outside of these number systems, let us look at matrices:

$$\left\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a,b\in\mathbb{Q}\right\}.$$

Note that this is a subring of $\mathbf{Mat}2(\mathbb{R})$.

[4.1.0.3] Definition (*Field*). A field $\mathbb{F}$ is a commutative ring with $1 \neq 0$ such that if $a \in \mathbb{F}$ and $a \neq 0$, then a is a unit.

[4.1.0.4] Definition (*Subfield*). If S is a subring of a field $\mathbb{F}$, and is also closed under multiplicative inverses of nonzero elements, then it is also a subfield.

We have previously learned that

$$\left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{Q} \right\}$$

is a subring of $\mathbf{Mat}2(\mathbb{R})$. But I also claim it is a field itself.

[4.1.0.5] Proposition. The set

$$\left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{Q} \right\}$$

is a field.

$\therefore$

Proof. Suppose

$$M = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

which means a and b are not both 0. Then

$$\det(M) = a^2 + b^2.$$

Since a and b are not both 0, we have $a^2 + b^2 \neq 0$. Thus

$$M^{-1} = \frac{1}{a^2 + b^2} \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

Since $a, b \in \mathbb{Q}$, this inverse is again of the same form with rational entries. Thus we have shown that the subring is also closed under multiplicative inverses of nonzero elements. This is a field. □

[4.1.0.6] Lemma. For n composite, $\mathbb{Z}_n$ is not a field if it has zero-divisors.

$\therefore$

Proof. If $\mathbb{Z}_n$ has a zero-divisor $[a] \neq [0]$, then there exists $[b] \neq [0]$ such that

$$[a][b] = [0].$$

If $\mathbb{Z}_n$ were a field, then $[a]$ would be a unit. Multiplying by $[a]^{-1}$ would give

$$[b] = [0],$$

a contradiction. Thus $\mathbb{Z}_n$ is not a field. □

From now on $\mathcal{R}, \mathcal{S}$ is a ring and $\mathbb{F}$ is a field.

[4.1.0.7] Definition (*Integral Domain*). Suppose $\mathcal{R}$ is a commutative ring with $1 \neq 0$. We say $\mathcal{R}$ is an integral domain if $a \neq 0$ and $a \in \mathcal{R}$ imply that a is not a zero-divisor.

We can think of these integral domain rings as being almost a field, but the only thing discerning them from being a field is the fact that not every nonzero element must have an inverse. The only zero-divisor is $0_{\mathcal{R}}$. Remember that if there is a nonzero zero-divisor in $\mathcal{R}$, then there is no way it can be a field, since all nonzero elements of a field must have an inverse, a.k.a. be a unit.

[4.1.0.8] Corollary. $\mathbb{F}$ is an integral domain.

$\therefore$

Proof. Suppose $a, b \in \mathbb{F}$ with $ab = 0$. Suppose $a \neq 0$. Then a is a unit with inverse a^{-1}. Then

$$\begin{aligned} a^{-1}(ab) &= a^{-1} \cdot 0 \\ (a^{-1}a)b &= 0 \\ 1b &= 0 \\ b &= 0. \end{aligned}$$

Thus if $ab = 0$, then $a = 0$ or $b = 0$. So $\mathbb{F}$ is an integral domain. □

Let us look into something called extensions.

[4.1.0.9] Definition (*Field Adjoins*). We call something an adjoin given that suppose we have $\mathbb{F} = \mathbb{Q}$. Note this field is a subfield of $\mathbb{R}$. Then an extension of $\mathbb{Q}$ is taking an element of $\mathbb{R} \setminus \mathbb{Q}$ and adding it to $\mathbb{Q}$. An example of this is

$$\mathbb{Q}\left[\sqrt{7}\right] := \{a + b\sqrt{7} : a, b \in \mathbb{Q}\}.$$

In fact, an exercise to do is to show that $\mathbb{Q}[\sqrt{7}]$ is a subfield. Based on everything we have observed, we can say that $\mathbb{Z}_p$ is a field and $\mathbb{Z}_n$ is not even an integral domain when n is composite.

[4.1.0.10] Axiom (*Pigeonhole Principle*). If you have $n+1$ objects in n slots, one slot will have more than 1 element.

[4.1.0.11] Theorem. A finite integral domain is a field.

$\therefore$

Proof. Let F be a finite integral domain. We need to show that if $0 \neq u \in F$, then u has a multiplicative inverse. Consider the set

$$\{u, u^2, u^3, \ldots\}.$$

Suppose F has n elements. Then there must be repetition, so $u^k = u^m$ for some $m > k$. Thus

$$u^m - u^k = 0$$

$$u^k(u^{m-k}-1)=0.$$

Since F is an integral domain, then $u^k=0$ or $u^{m-k}-1=0$. Since $u\neq 0$, we must have $u^k\neq 0$. Then

$$\begin{aligned} u^{m-k}-1&=0\\ u^{m-k}&=1\\ u(u^{m-k-1})&=1. \end{aligned}$$

Thus $u^{-1}=u^{m-k-1}$. So every nonzero element of F has a multiplicative inverse. Therefore F is a field. □

4.2 Homomorphisms and Isomorphisms

[4.2.0.1] Definition (*Homomorphism*). Let $\mathcal{R}$ and $\mathcal{S}$ be rings. Suppose a function $f:\mathcal{R}\to\mathcal{S}$ is given. If for all $a,b\in\mathcal{R}$,

$$f(a+b)=f(a)+f(b)$$

and

$$f(ab)=f(a)f(b),$$

then f is called a homomorphism.

[4.2.0.2] Definition (*Isomorphism*). Suppose $f:\mathcal{R}\to\mathcal{S}$ is a bijective homomorphism. Then f is called an isomorphism.

If f is an isomorphism, then $\mathcal{R}$ and $\mathcal{S}$ are isomorphic to each other. Suppose $\mathcal{R}=\mathbb{Z}$ and $\mathcal{S}=2\mathbb{Z}$, and let $f:\mathcal{R}\to\mathcal{S}$ be defined by $f(m)=2m$. Is this an isomorphism?

[4.2.0.3] Example. We compute

$$f(m+n)=2(m+n)=2m+2n=f(m)+f(n).$$

So f preserves addition. However,

$$f(mn)=2mn,$$

while

$$f(m)f(n)=(2m)(2n)=4mn.$$

Thus

$$f(mn)\neq f(m)f(n)$$

in general. So f is not a ring homomorphism. Hence $\mathbb{Z}$ and $2\mathbb{Z}$ are not isomorphic by this map.

[4.2.0.4] Definition (*Endomorphism*). A homomorphism that maps $\mathcal{R}$ to itself is called an endomorphism.

[4.2.0.5] Definition (*Automorphism*). An isomorphic endomorphism is called an automorphism.

[4.2.0.6] Proposition. A function is bijective if and only if it has an inverse.

$\therefore$

Proof. First suppose $f : \mathcal{R} \to \mathcal{S}$ has an inverse function $g : \mathcal{S} \to \mathcal{R}$. Then

$$g \circ f = \mathrm{id}_{\mathcal{R}}$$

and

$$f \circ g = \mathrm{id}_{\mathcal{S}}.$$

Hence f is injective and surjective, so f is bijective. Conversely, suppose f is bijective. Since f is surjective, for every $y \in \mathcal{S}$ there exists $x \in \mathcal{R}$ such that $f(x) = y$. Since f is injective, this x is unique. So we may define a function $g : \mathcal{S} \to \mathcal{R}$ by letting $g(y) = x$, where $f(x) = y$. Then

$$g \circ f = \mathrm{id}_{\mathcal{R}}$$

and

$$f \circ g = \mathrm{id}_{\mathcal{S}}.$$

Thus g is an inverse of f. □

[4.2.0.7] Axiom (*Isomorphism Properties*). We can check some properties of a homomorphism to rule out whether two rings are isomorphic. In particular, isomorphic rings must have the same:

1. number of elements, when finite;
2. number of units;
3. number of zero-divisors.

These are useful necessary checks, though by themselves they do not always prove two rings are isomorphic.

For example, we can state that $\mathbb{Z} \ncong q$. The reason is that every nonzero element in q is a unit, while the only units in $\mathbb{Z}$ are ± 1. Similarly, $\mathbb{Z}_4 \ncong \mathbb{Z}_6$, due to the number of elements.

Perhaps in previous courses, such as Calculus III, you have looked at $\mathbb{R}^3$, which means a 3-tuple ordered triple that represents (x, y, z) in space. However, this is a generalized fact. What if I wanted to have two points from different sets, but still create an ordered pair or tuple?

[4.2.0.8] Axiom (*Cartesian Product*). If $\mathcal{R}$ and $\mathcal{S}$ are rings, then

$$\mathcal{R} \times \mathcal{S} := \{(r, s) : r \in \mathcal{R},\ s \in \mathcal{S}\}$$

is also a ring under addition and multiplication defined by

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2),$$
$$(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

It will be a fun exercise to prove the following lemma, or at least work through a couple of examples.

[4.2.0.9] Lemma. If $\gcd(m, n) = 1$, then

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}.$$

$\therefore$

Proof. □

Note that in $\mathbb{Z} \times \mathbb{Z}$, the zero-divisors include $(0, 1)$ and $(1, 0)$. Let $\mathcal{R} = \mathcal{S} = \mathbb{Z}$ in $\mathbb{Z} \times \mathbb{Z}$. Let $\pi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be the projection map onto the first coordinate. Then

$$\pi((1, 0)) = 1,$$

which is a unit. So a homomorphism need not preserve zero-divisors.

Chapter 5

Polynomials

5.1 Polynomials

[5.1.0.1] Definition (*Polynomial*). A polynomial with coefficients in $\mathcal{R}$ is denoted by $\mathcal{R}[x]$. It consists of expressions of the form

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$

where $a_i \in \mathcal{R}$. We can think of the a_i as coefficients.

[5.1.0.2] Proposition. Addition and multiplication in $\mathcal{R}[x]$ are defined component-wise.

$\therefore$

Proof. Let

$$f(x) = a_0 + \ldots + a_n x^n,$$
$$g(x) = b_0 + \ldots + b_m x^m,$$

where $m \geq n$. Then

$$f(x) + g(x) = (a_0 + b_0) + \ldots + (a_n + b_n)x^n + b_{n+1}x^{n+1} + \ldots + b_m x^m.$$

Multiplication is defined by distributing and collecting like terms. □

This informal definition raises several questions. What is x? Is it an element of $\mathcal{R}$? If not, what does it mean to multiply x by a ring element? To answer these questions, note that an expression of the form

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

makes sense provided that the a_i and x are all elements of some larger ring. An analogy might be helpful here. The number π is not in the ring of integers $\mathbb{Z}$, but expressions such as

$$3 - 4\pi + 12\pi^2 + \pi^3$$

make sense in $\mathbb{R}$. Furthermore, it is not difficult to verify that the set of all numbers of the form

$$\sum_{i=0}^{n} a_i \pi^i,$$

with $n \geq 0$ and $a_i \in \mathbb{Z}$, is a subring of $\mathbb{R}$ that contains both $\mathbb{Z}$ and π. For the present, we shall think of polynomials with coefficients in a ring $\mathcal{R}$ in much the same way, as elements of a larger ring that contains both $\mathcal{R}$ and a special element x that is not in $\mathcal{R}$. Feel free to check that $\mathcal{R}[x]$ is a ring, but we will be concentrating on $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x], \mathbb{Z}_p[x]$, and have their elements denoted by $f(x)$ or $P(x)$.

[5.1.0.3] Definition (*Degree of a Polynomial*). If $f(x) \in \mathcal{R}[x]$, the degree of $f(x)$, denoted by $\deg f(x)$, is the largest n for which the coefficient of x^n is not 0. The coefficient a_n is called the leading coefficient.

[5.1.0.4] Definition (*Additive Identity of $\mathcal{R}[x]$*). The additive identity in $\mathcal{R}[x]$ is the zero polynomial, where all coefficients are 0.

If $\deg f(x) = 0$, then $f(x)$ is a constant polynomial.

[5.1.0.5] Proposition (*Degree Arithmetic*). Suppose $\deg f(x) = m$ and $\deg g(x) = n$.

$\therefore$

Proof.

$$\deg(f(x) + g(x)) \leq \max\{m, n\}.$$

If $m \neq n$, then

$$\deg(f(x) + g(x)) = \max\{m, n\}.$$

If $m = n$, then

$$\deg(f(x) + g(x)) \leq m,$$

with equality unless cancellation occurs. Also,

$$\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x).$$

If $\mathcal{R}$ is an integral domain, then

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x).$$

□

Let $f(x), g(x) \in \mathbb{Z}_4[x]$. Let $f(x) = 2x$ and $g(x) = 2x^2$. Then

$$f(x)g(x) = 4x^3 = 0.$$

From now on $\mathcal{R}$ is an Integral Domain.

Given that $\mathcal{R}$ is an integral domain, one may naturally ask what are the units of $\mathcal{R}[x]$.

[5.1.0.6] Lemma. Suppose $u(x)$ is a unit with multiplicative inverse $v(x)$. Then

$$u(x)v(x) = 1 = 1 + 0x + 0x^2 + \dots.$$

∴

Proof. □

5.2 Division

[5.2.0.1] Theorem (*Division Algorithm in Polynomial Fields*). Suppose $\mathbb{F}$ is a field and $a(x), b(x) \in \mathbb{F}[x]$ with $b(x) \neq 0$. Then there exist unique $q(x), r(x) \in \mathbb{F}[x]$ such that

$$a(x) = q(x)b(x) + r(x)$$

with $\deg(r(x)) < \deg(b(x))$ or $r(x) = 0$.

∴

Proof. **Case 1:** If $a(x) = 0$ or $\deg(a(x)) < \deg(b(x))$, then let

$$q(x) = 0, \qquad r(x) = a(x).$$

Then

$$a(x) = b(x) \cdot 0 + a(x),$$

so the conclusion holds. **Case 2:** Suppose $a(x) \neq 0$ and $\deg(a(x)) \geq \deg(b(x))$. Write

$$a(x) = a_n x^n + \dots, \qquad b(x) = b_m x^m + \dots$$

with $a_n, b_m \neq 0$ and $n \geq m$. Since $\mathbb{F}$ is a field, b_m^{-1} exists. Let

$$h(x) := a(x) - a_n b_m^{-1} x^{n-m} b(x).$$

Then the leading terms cancel, so

$$\deg(h(x)) < \deg(a(x)).$$

By strong induction on $\deg(a(x))$, there exist $q_1(x), r(x) \in \mathbb{F}[x]$ such that

$$h(x) = q_1(x)b(x) + r(x)$$

with $\deg(r(x)) < \deg(b(x))$ or $r(x) = 0$. Therefore

$$\begin{aligned} a(x) &= a_n b_m^{-1} x^{n-m} b(x) + h(x) \\ &= a_n b_m^{-1} x^{n-m} b(x) + q_1(x)b(x) + r(x) \\ &= (a_n b_m^{-1} x^{n-m} + q_1(x))b(x) + r(x). \end{aligned}$$

So if we let

$$q(x) := a_n b_m^{-1} x^{n-m} + q_1(x),$$

then

$$a(x) = q(x)b(x) + r(x)$$

with $\deg(r(x)) < \deg(b(x))$ or $r(x) = 0$.

Proof of Uniqueness: Suppose

$$\begin{aligned} a(x) &= q_1(x)b(x) + r_1(x) \\ &= q_2(x)b(x) + r_2(x), \end{aligned}$$

where $\deg(r_1(x)), \deg(r_2(x)) < \deg(b(x))$ or $r_1(x) = r_2(x) = 0$. Then

$$\begin{aligned} [q_1(x) - q_2(x)]b(x) + [r_1(x) - r_2(x)] &= 0, \\ [q_1(x) - q_2(x)]b(x) &= r_2(x) - r_1(x). \end{aligned}$$

Now either $r_2(x) - r_1(x) = 0$, or

$$\deg(r_2(x) - r_1(x)) < \deg(b(x)).$$

If $(q_1(x) - q_2(x))b(x) \neq 0$, then since $\mathbb{F}[x]$ is an integral domain,

$$\deg((q_1(x) - q_2(x))b(x)) = \deg(q_1(x) - q_2(x)) + \deg(b(x)) \geq \deg(b(x)).$$

This is impossible, since the right-hand side has degree strictly less than $\deg(b(x))$ or is 0. Therefore

$$(q_1(x) - q_2(x))b(x) = 0.$$

Hence $q_1(x) = q_2(x)$. Then

$$r_2(x) - r_1(x) = 0,$$

so $r_1(x) = r_2(x)$. □

The Division Algorithm for polynomial fields is a fundamental concept that allows you to divide one polynomial by another, similar to the division algorithm with integers. This algorithm helps you express one polynomial as a quotient of another polynomial plus a remainder.

[5.2.0.2] Definition (*Logical Divide of Polynomial Fields*). Let $a(x), b(x) \in \mathbb{F}[x]$ and $b(x) \neq 0$. We say $b(x) \mid a(x)$ if there exists a $q(x) \in \mathbb{F}[x]$ such that

$$a(x) = q(x)b(x).$$

[5.2.0.3] Definition (*GCD of Polynomial Fields*). Suppose $a(x), b(x) \in \mathbb{F}[x]$ are not both 0. We say $d(x) = \gcd(a(x), b(x))$ if $d(x) \mid a(x)$, $d(x) \mid b(x)$, and whenever $c(x) \in \mathbb{F}[x]$ satisfies $c(x) \mid a(x)$ and $c(x) \mid b(x)$, then $c(x) \mid d(x)$.

Suppose we are in $\mathbb{Q}[x]$. Let

$$a(x) = (x-1)^2$$

and

$$b(x) = (x-1)(x-2).$$

Then $\gcd(a(x), b(x)) = x - 1$. But wait, does not $2x - 2 \mid a(x)$ and $b(x)$ as well. We have a problem on our hands. We have to figure out how to circumvent this solution, and before we can do that, let us go ahead and introduce a new term.

[5.2.0.4] Definition (*Monic*). If $d(x) \in \mathbb{F}[x]$ has leading coefficient 1, then $d(x)$ is monic.

In algebra, monic polynomials are commonly used in the context of irreducible polynomials. Monic irreducible polynomials have leading coefficient 1, and this condition simplifies discussions of unique factorization.

[5.2.0.5] Definition (*Polynomial Associates*). If $c(x), d(x) \in \mathbb{F}[x]$ and

$$c(x) = \beta d(x)$$

for some $\beta \in \mathbb{F}$ with $\beta \neq 0$, we say $c(x)$ and $d(x)$ are associates.

We can think of associates as polynomial constant multiples.

[5.2.0.6] Theorem (*GCD Theorem*). Suppose $a(x), b(x) \in \mathbb{F}[x]$ are not both 0. Let

$$S := \{u(x)a(x) + v(x)b(x) \neq 0 : u(x), v(x) \in \mathbb{F}[x]\}.$$

Then there exist $u(x), v(x) \in \mathbb{F}[x]$ such that

$$d(x) = u(x)a(x) + v(x)b(x)$$

and $d(x) = \gcd(a(x), b(x))$. Moreover, S has a unique monic polynomial of smallest degree, and this polynomial is $\gcd(a(x), b(x))$.

$\therefore$

Proof. This theorem also answers the question to our gcd question, which shows that we want to have a monic polynomial of smallest degree as our $\gcd(a(x), b(x))$. The set of degrees is a subset of $\mathbb{Z}^{\geq 0}$, so let $d(x)$ be a monic polynomial of minimal degree in S. We need to show that $d(x) \mid a(x)$. Using the division algorithm, write

$$a(x) = q(x)d(x) + r(x),$$

where $r(x) = 0$ or $\deg(r(x)) < \deg(d(x))$. Now since $d(x) \in S$, there exist $u(x), v(x) \in \mathbb{F}[x]$ such that

$$d(x) = u(x)a(x) + v(x)b(x).$$

So

$$\begin{aligned} r(x) &= a(x) - q(x)d(x) \\ &= a(x) - q(x)(u(x)a(x) + v(x)b(x)) \\ &= (1 - q(x)u(x))a(x) - q(x)v(x)b(x). \end{aligned}$$

Thus if $r(x) \neq 0$, then $r(x) \in S$. But then

$$\deg(r(x)) < \deg(d(x)),$$

contradicting the fact that $d(x)$ has the least degree among nonzero elements of S. So $r(x) = 0$, and hence $d(x) \mid a(x)$. Similarly, $d(x) \mid b(x)$. Now suppose $c(x) \mid a(x)$ and $c(x) \mid b(x)$. Then $c(x)$ divides every linear combination of $a(x)$ and $b(x)$. In particular,

$$c(x) \mid u(x)a(x) + v(x)b(x) = d(x).$$

Therefore $d(x) = \gcd(a(x), b(x))$. Finally, gcds are unique up to associates, and among all associates there is exactly one monic polynomial. Hence the monic gcd is unique. □

This theorem also answers the question to our gcd question, which shows that we want to have a monic polynomial of smallest degree as our $\gcd(a(x), b(x))$. The GCD Theorem for polynomial fields is a fundamental result in abstract algebra that addresses the existence and uniqueness of the greatest common divisor of two polynomials in a polynomial ring over a field. The theorem establishes a clear and precise method for finding the gcd of polynomials and its properties.

[5.2.0.7] Definition (*Relatively Prime*). Suppose $a(x), b(x) \in \mathbb{F}[x]$ are not both 0. We say $a(x)$ and $b(x)$ are relatively prime if

$$\gcd(a(x), b(x)) = 1.$$

[5.2.0.8] Corollary (*Consequence of GCD Theorem*). Suppose $a(x), b(x) \in \mathbb{F}[x]$ are relatively prime and $c(x) \in \mathbb{F}[x]$. If $a(x) \mid b(x)c(x)$, then $a(x) \mid c(x)$.

∴

Proof. By the gcd theorem, we have

$$1 = u(x)a(x) + v(x)b(x)$$

for some $u(x), v(x) \in \mathbb{F}[x]$. Thus

$$c(x) = c(x)u(x)a(x) + c(x)v(x)b(x).$$

Since $a(x) \mid c(x)u(x)a(x)$ and $a(x) \mid c(x)v(x)b(x)$, it follows that

$$a(x) \mid c(x).$$

□

If we let $\mathcal{R} = \mathbb{F}[x]$, we notice that it has very similar properties to $\mathbb{Z}$, such that it has the division and gcd algorithm. In fact, it also will have relatively prime and an equivalence to primes, but for polynomials. Let us look at this equivalence.

[5.2.0.9] Definition (*Irreducible*). A polynomial $p(x) \in \mathbb{F}[x]$ is irreducible if whenever

$$p(x) = a(x)b(x)$$

for $a(x), b(x) \in \mathbb{F}[x]$, then $a(x)$ is an associate of $p(x)$ or $a(x)$ is a unit.

5.3 Irreducibility

[5.3.0.1] Proposition (*Polynomial Euclid's Lemma*). Suppose $p(x) \in \mathbb{F}[x]$ is irreducible and $b(x) \in \mathbb{F}[x]$ such that $p(x) \nmid b(x)$. Then

$$\gcd(p(x), b(x)) = 1.$$

$\therefore$

Proof. Let $d(x) = \gcd(p(x), b(x))$. Then

$$d(x) \mid p(x), \qquad d(x) \mid b(x).$$

Since $p(x)$ is irreducible, every divisor of $p(x)$ is either a unit or an associate of $p(x)$. Because gcds are taken to be monic, $d(x)$ is monic. Hence either $d(x) = 1$, or $d(x) = cp(x)$ for some nonzero $c \in \mathbb{F}$. If $d(x) = cp(x)$, then since $d(x) \mid b(x)$, it follows that $p(x) \mid b(x)$, which is a contradiction. Therefore

$$\gcd(p(x), b(x)) = 1.$$

□

[5.3.0.2] Corollary. If $p(x) \mid a_1(x) \cdots a_n(x)$, where $a_i(x) \in \mathbb{F}[x]$ and $p(x)$ is irreducible, then $p(x) \mid a_i(x)$ for some i.

$\therefore$

Proof. Show this by induction on n. □

[5.3.0.3] Theorem. Suppose $a(x) \in \mathbb{F}[x]$. Then $a(x)$ has a factorization into irreducible polynomials. This factorization is unique up to order and associates.

$\therefore$

Proof. Use strong induction on $\deg(a(x))$ for existence.

For uniqueness, suppose

$$\begin{aligned} a(x) &= p_1(x) \dots p_r(x) \\ &= q_1(x) \dots q_s(x), \end{aligned}$$

where each $p_i(x)$ and $q_j(x)$ is irreducible. Then

$$p_1(x) \mid q_1(x) \cdots q_s(x).$$

By the previous corollary,

$$p_1(x) \mid q_j(x)$$

for some j. Without loss of generality, after rearranging, assume $j = 1$. Since $q_1(x)$ is irreducible, $p_1(x)$ and $q_1(x)$ are associates. Proceed by induction on $\min\{r, s\}$. □

[5.3.0.4] Lemma (*Irreducible Degrees*). Degree 1 polynomials are irreducible. If a degree 2 polynomial is reducible, then it is a product of linear polynomials.

∴

Proof. □

[5.3.0.5] Lemma (*Freshman's Dream*). In $\mathbb{Z}_2$,

$$(x+1)^2 = x^2 + 1.$$

∴

Proof. □

[5.3.0.6] Proposition. If $f(x)$ is irreducible in $\mathbb{F}[x]$, then so is every associate of $f(x)$.

∴

Proof. □

Take note that for the equation $x^2 + ax + b$, there are p choices for each of a, b in $\mathbb{Z}_p$, which means p^2 total monic choices for this polynomial. More generally, the number of monic polynomials of degree n in $\mathbb{Z}_p[x]$ is p^n. The total number of polynomials of degree n is

$$(p-1)p^n.$$

[5.3.0.7] Example. Prove that $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$.

Proof. We have

$$x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right) \in \mathbb{R}[x].$$

If $x^2 - 2$ factored in $\mathbb{Q}[x]$, then since it has degree 2, it would factor into linear polynomials over $\mathbb{Q}$. That would force it to have a rational root. But its roots are $\pm\sqrt{2}$, and $\sqrt{2} \notin q$. Therefore $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$. ■

Let $\mathbb{F}$ be a field. Take $f(x) \in \mathbb{F}[x]$. There is a corresponding polynomial function $\mathbb{F} \to \mathbb{F}$ also denoted by $f(x)$.

[5.3.0.8] Theorem (*Factor Theorem*). Let $f(x) \in \mathbb{F}[x]$ and $a \in \mathbb{F}$. If $f(a) = 0$, then $(x - a)$ is a factor of $f(x)$. That is,

$$f(x) = g(x)(x - a)$$

for some $g(x) \in \mathbb{F}[x]$.

∴

Proof. □

[5.3.0.9] Example. (a) Show that x^2+2 is irreducible in $\mathbb{Z}_5[x]$.

Proof. We will do a proof by contradiction. Suppose x^2+2 is reducible in $\mathbb{Z}_5[x]$. Since it has degree 2, it must factor into linear polynomials:

$$x^2+2=(x+a)(x+b)$$

for some $a,b\in\mathbb{Z}_5$. Expanding gives

$$(x+a)(x+b)=x^2+(a+b)x+ab.$$

Since there is no degree 1 term in x^2+2, we must have

$$a+b=0,$$

so $b=-a$. Then

$$(x+a)(x-a)=x^2-a^2.$$

Thus we would need

$$-a^2=2$$

in $\mathbb{Z}_5$, equivalently

$$a^2=3.$$

But the squares in $\mathbb{Z}_5$ are

$$0^2=0,\quad 1^2=1,\quad 2^2=4,\quad 3^2=4,\quad 4^2=1.$$

So 3 is not a square in $\mathbb{Z}_5$. This is a contradiction. Therefore x^2+2 is irreducible in $\mathbb{Z}_5[x]$. ■

(b) Factor x^4-4 as a product of irreducible in $\mathbb{Z}_5[x]$.

We have

$$x^4-4=(x^2+2)(x^2-2).$$

Now in $\mathbb{Z}_5$, we have $-2\equiv 3$. Since 4 is a square in $\mathbb{Z}_5$, $x^2-2=x^2+3$ is reducible. Indeed,

$$x^2-2=x^2+3=(x-1)(x+1).$$

Also, from part (a), x^2+2 is irreducible. Thus

$$x^4-4=(x^2+2)(x-1)(x+1)$$

is a factorization into irreducible in $\mathbb{Z}_5[x]$.

[5.3.0.10] Theorem (*Remainder Theorem*). Let $f(x)\in\mathbb{F}[x]$ and $a\in\mathbb{F}$. Then

$$f(x)=g(x)(x-a)+r(x)$$

for some $g(x)\in\mathbb{F}[x]$, where $r(x)$ is a constant polynomial.

∴

Proof. □

Proof. By the division algorithm,

$$f(x)=g(x)(x-a)+r(x),$$

where $r(x) = 0$ or

$$\deg(r(x)) < \deg(x-a) = 1.$$

Thus $r(x)$ must be a constant polynomial or 0. ■

Proof. By the remainder theorem,

$$f(x) = g(x)(x-a) + r$$

where r is a constant. Evaluating at $x = a$ gives

$$\begin{aligned} f(a) &= g(a)(a-a) + r \\ &= r. \end{aligned}$$

So if $f(a) = 0$, then $r = 0$. Hence

$$f(x) = g(x)(x-a).$$

■

[5.3.0.11] Definition (*Roots*). a is a root of $f(x)$ if

$$f(a) = 0.$$

[5.3.0.12] Corollary (*of Factor Theorem*). Suppose $f(x) \in \mathbb{F}[x]$ has $\deg f(x) = n$. Then $f(x)$ has at most n different roots.

∴

Proof. By induction on $\deg f(x)$. If $\deg f(x) = 0$, then f is a nonzero constant and has no roots. If $\deg f(x) = 1$, then

$$f(x) = a_1 x + a_0, \qquad a_1 \neq 0.$$

It has exactly one root, namely

$$x = \frac{-a_0}{a_1}.$$

Assume true for polynomials of degree $n-1$. Now let $\deg f(x) = n$ and suppose a is a root of $f(x)$. Then by the factor theorem,

$$f(x) = (x-a)g(x)$$

for some $g(x)$ with $\deg g(x) = n-1$. If $b \neq a$ is another root of $f(x)$, then

$$0 = f(b) = (b-a)g(b).$$

Since $b - a \neq 0$, we get $g(b) = 0$. Thus every root of $f(x)$ other than a is a root of $g(x)$. By the induction hypothesis, there are at most $n-1$ such roots. So the number of roots of $f(x)$ is at most

$$1 + (n-1) = n.$$

□

If $f(x) \in \mathbb{Q}[x]$, then the rational root test tells us if $f(x)$ has a linear factor.

[5.3.0.13] Definition (*Rational Root Test*). Suppose

$$f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x].$$

If $\frac{r}{s} \in q$ in lowest terms is a root of $f(x)$, then

$$r \mid a_0 \qquad \text{and} \qquad s \mid a_n.$$

Since a_0 and a_n have finitely many divisors, there are only finitely many possibilities to check.

For example, $2x^3 - x^2 + 1$ is irreducible by the rational root test, since the only possible rational roots are

$$\pm 1, \ \pm\frac{1}{2}.$$

After checking all possibilities, none of them are roots. Suppose $f(x) \in \mathbb{Z}[x]$ and $g(x), h(x) \in q_{[}x]$. Then there exist $\alpha, \beta \in q$ such that

$$f(x) = (\alpha g(x))(\beta h(x)) \in \mathbb{Z}[x].$$

Also, if $f(x) \in q_{[}x]$, then there is a $c \in q$ such that $cf(x) \in \mathbb{Z}[x]$. The rational root test tells us about linear factors, which suffices to show irreducibility for degrees 2 and 3, but not in higher degrees. This builds the foundation for the following theorem.

[5.3.0.14] Theorem (*Gauss's Lemma of Irreducibility*). Suppose $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is irreducible in $\mathbb{Z}[x]$, then $f(x)$ is irreducible in $q_{[}x]$.

$\therefore$

Proof. □

One may ask whether the converse is possible given these assumptions. I claim not always. It is possible when primitivity is included. This course will not go deeply into primitivity, but here is the definition.

[5.3.0.15] Definition (*Primitivity*). A polynomial $p(x)$ with integer coefficients is called primitive if and only if the gcd of all its coefficients is 1.

If this is also true, then and only then do we get the full biconditional statement. This was a whole block of assumptions to unfold before displaying the if-then statement of Gauss's lemma of irreducibility. But let us look at an example of how to apply this.

Let

$$f(x) = 6x^2 - 5x + 1.$$

Then

$$f(x) = \left(x - \frac{1}{2}\right)(6x - 2),$$

so

$$f\left(\frac{1}{2}\right) = 0.$$

Thus we have shown a root in $q_{[}x]$, which demonstrates that it is reducible. But we can also write

this in the form of integer factors:

$$f(x) = (2x-1)(3x-1) \in \mathbb{Z}[x].$$

[5.3.0.16] Lemma (*Introductory Lemma*). Suppose $f(x), g(x), h(x) \in \mathbb{Z}[x]$ where

$$f(x) = g(x)h(x).$$

Let p be prime such that p divides every coefficient of $f(x)$. Then either p divides every coefficient of $g(x)$ or p divides every coefficient of $h(x)$.

$\therefore$

Proof. □

Proof. Suppose

$$f(x) = g(x)h(x),$$

with

$$f(x) = a_0 + a_1 x + \ldots, \quad g(x) = b_0 + b_1 x + \ldots, \quad h(x) = c_0 + c_1 x + \ldots.$$

Then

$$a_0 = b_0 c_0.$$

Since $p \mid a_0$, by Euclid's lemma we get

$$p \mid b_0 \qquad \text{or} \qquad p \mid c_0.$$

Assume without loss of generality that $p \nmid c_0$. We will show by induction that $p \mid b_i$ for all i. Now

$$a_1 = b_0 c_1 + b_1 c_0.$$

Since $p \mid a_1$ and $p \mid b_0 c_1$, it follows that $p \mid b_1 c_0$. Because $p \nmid c_0$, we conclude $p \mid b_1$. Continuing this argument inductively shows that p divides every coefficient of $g(x)$. ■

[5.3.0.17] Theorem (*Eisenstein's Theorem of Irreducibility*). Suppose

$$f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x].$$

Suppose $p \nmid a_n$, $p \mid a_i$ for all $i < n$, and $p^2 \nmid a_0$. Then $f(x)$ is irreducible in $q_{[}x]$.

$\therefore$

Proof. Suppose $f(x)$ is reducible in $q_{[}x]$. Then by Gauss's lemma, $f(x)$ is reducible in $\mathbb{Z}[x]$. So

$$f(x) = g(x)h(x),$$

where $g(x), h(x) \in \mathbb{Z}[x]$ and

$$\deg g(x), \deg h(x) < \deg f(x) = n.$$

Using the introductory lemma and tracking the divisibility of coefficients by p, one concludes that p must divide every coefficient of one factor. Then p^2 divides the constant term a_0, contradicting the hypothesis. Therefore $f(x)$ is irreducible in $q_{[}x]$. □

[5.3.0.18] Lemma. Linear polynomials are not reducible.

∴

Proof. A linear polynomial cannot be written as a product of two non-unit polynomials, since degrees add under multiplication and both non-unit factors would have positive degree. □

Let

$$f(x) = 2x^4 + 15x^3 + 30x^2 + 60x - 21.$$

We have

$$3 \nmid 2, \qquad 3 \mid 15, 30, 60, 21, \qquad 9 \nmid 21.$$

So $f(x)$ is irreducible by Eisenstein.

[5.3.0.19] Theorem (*Reduction mod p*). Let $f(x) \in \mathbb{Z}[x]$. Let $p \nmid a_n$, where a_n is the leading coefficient of $f(x)$. Consider

$$\overline{f(x)} = \overline{a_n}x^n + \ldots + \overline{a_0},$$

where $\overline{a_i}$ is the congruence class of $a_i \mod p$. If $\overline{f(x)}$ is irreducible in $\mathbb{Z}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$ and $q_[x]$. The converse is not true.

∴

Proof. Suppose $f(x)$ is reducible in $\mathbb{Z}[x]$. Then

$$f(x) = g(x)h(x)$$

for some $g(x), h(x) \in \mathbb{Z}[x]$ of smaller positive degree. Reducing mod p gives

$$\overline{f(x)} = \overline{g(x)}\,\overline{h(x)}.$$

Since $p \nmid a_n$, the degree of $\overline{f(x)}$ is still n, so both $\overline{g(x)}$ and $\overline{h(x)}$ have smaller degree than $\overline{f(x)}$. This contradicts the irreducibility of $\overline{f(x)}$ in $\mathbb{Z}_p[x]$. So $f(x)$ is irreducible in $\mathbb{Z}[x]$. Then by Gauss's lemma, $f(x)$ is irreducible in $q_[x]$. □

Let

$$f(x) = x^4 + 3x^3 + 6x^2 + 1 \in \mathbb{Q}[x].$$

Try $p = 2$. Then

$$\overline{f(x)} = x^4 + x^3 + 1.$$

It has no roots in $\mathbb{Z}_2$, so it has no linear factors. Hence it is irreducible in $\mathbb{Z}_2[x]$, and therefore $f(x)$ is irreducible in $\mathbb{Q}[x]$.

[5.3.0.20] Theorem (*Fundamental Theorem of Algebra*). If $f(x) \in \mathbb{C}[x]$, then the following are equivalent:

1. $f(x)$ is irreducible;
2. $f(x)$ is linear;
3. every non-constant polynomial in $\mathbb{C}[x]$ can be factored as a product of linear factors;

4. every non-constant polynomial in $\mathbb{C}[x]$ has a root.

$\therefore$

Proof. □

For example,

$$f(x) = x^2 + 1 \in \mathbb{C}[x]$$

has complex roots $\pm i$, and

$$f(x) = (x+i)(x-i).$$

Let $\theta = \frac{2\pi}{3}, \frac{4\pi}{3}$. Then

$$\begin{aligned} e^{\theta i} &= \cos\theta + i\sin\theta, \\ \left(e^{\theta i}\right)^3 &= \cos 3\theta + i\sin 3\theta \\ &= \cos 2\pi + i\sin 2\pi \\ &= \cos 4\pi + i\sin 4\pi \\ &= 1. \end{aligned}$$

Roots of $x^n - 1$ are

$$e^{\theta i}, e^{2\theta i}, e^{3\theta i}, \ldots, e^{(n-1)\theta i}.$$

[5.3.0.21] Proposition. Suppose $f(x) \in \mathbb{R}[x]$. Every irreducible polynomial in $\mathbb{R}[x]$ has degree 1 or 2.

$\therefore$

Proof. Consider $f(x) \in \mathbb{R}[x]$ as a polynomial in $\mathbb{C}[x]$. By the Fundamental Theorem of Algebra, $f(x)$ has a root in $\mathbb{C}$. If this root is real, then $f(x)$ has a linear factor. So assume the root is

$$\omega = a + bi$$

with $b \neq 0$. Then $\overline{\omega} = a - bi$ is also a root. Indeed, since the coefficients of $f(x)$ are real, complex conjugation fixes each coefficient, and thus

$$f(\omega) = 0 \implies f(\overline{\omega}) = 0.$$

Therefore

$$(x-\omega)(x-\overline{\omega})$$

is a factor of $f(x)$. But

$$(x-\omega)(x-\overline{\omega}) = x^2 - (\omega + \overline{\omega})x + \omega\overline{\omega},$$

and

$$\omega + \overline{\omega} \in \mathbb{R}, \qquad \omega\overline{\omega} \in \mathbb{R}.$$

So this quadratic factor lies in $\mathbb{R}[x]$. Hence every irreducible polynomial in $\mathbb{R}[x]$ has degree 1 or 2. □

[5.3.0.22] Example. Suppose $f(x) \in \mathbb{R}[x]$ and has degree 3. By the Intermediate Value Theorem, there exists $c \in \mathbb{R}$ such that $f(c) = 0$. So by the factor theorem, $(x - c)$ is a factor of $f(x) \in \mathbb{R}[x]$.

[5.3.0.23] Lemma. Now let $\varphi(a + bi) = a - bi$. Then $\varphi : \mathbb{C} \to \mathbb{C}$ is an isomorphism.

$\therefore$

Proof. □

5.4 Congruences Revisited

[5.4.0.1] Definition (*Congruences*). Let $m(x) \in \mathbb{F}[x]$ with $m(x) \neq 0$. If $a(x), b(x) \in \mathbb{F}[x]$, we define

$$a(x) \equiv b(x) \mod m(x)$$

if

$$m(x) \mid a(x) - b(x).$$

Equivalently, there exists $q(x) \in \mathbb{F}[x]$ such that

$$a(x) - b(x) = q(x)m(x).$$

Equivalently,

$$a(x) = b(x) + q(x)m(x).$$

[5.4.0.2] Definition (*Congruence Class*). The congruence class of $a(x) \in \mathbb{F}[x]$ is denoted by $[a(x)]$. It consists of

$$[a(x)] := \{b(x) \in \mathbb{F}[x] : b(x) \equiv a(x) \mod m(x)\}.$$

[5.4.0.3] Definition (*Polynomial Division Algorithm*). Suppose $g(x) \in \mathbb{F}[x]$. Then

$$g(x) = q(x)m(x) + r(x),$$

where $\deg r(x) < \deg m(x)$ or $r(x) = 0$. Since

$$g(x) - r(x) = q(x)m(x),$$

we have

$$r(x) \equiv g(x) \mod m(x).$$

So $g(x) \in [r(x)]$. Thus every $g(x)$ is in exactly one of these congruence classes.

[5.4.0.4] Lemma. In $\mathbb{Z}_p[x]$, if $\deg m(x) = n$, then there are exactly p^n different congruence classes modulo $m(x)$.

$\therefore$

Proof. Every polynomial is congruent modulo $m(x)$ to exactly one polynomial of degree less than n or to 0. Such a representative has the form

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1},$$

where each coefficient is in $\mathbb{Z}_p$. There are p choices for each coefficient, and there are n coefficients. So there are exactly

$$p^n$$

such polynomials. Hence there are exactly p^n distinct congruence classes. □

Similar to congruence classes in the integers, we also have similar ideas for addition and multiplication for polynomial congruences.

[5.4.0.5] Definition (*Modular Operations*). Addition is defined by

$$[a(x)] + [b(x)] := [a(x) + b(x)].$$

Multiplication is defined by

$$[a(x)][b(x)] := [a(x)b(x)].$$

We can use this to check that these operations are well-defined.

[5.4.0.6] Lemma (*Well-Defined*). Suppose $[a(x)] = [c(x)]$ and $[b(x)] = [d(x)]$. Then:

1. $[a(x) + b(x)] = [c(x) + d(x)]$;
2. $[a(x)b(x)] = [c(x)d(x)]$.

$\therefore$

Proof. Since $[a(x)] = [c(x)]$, we have

$$a(x) \equiv c(x) \mod m(x).$$

Since $[b(x)] = [d(x)]$, we have

$$b(x) \equiv d(x) \mod m(x).$$

Thus

$$m(x) \mid a(x) - c(x)$$

and

$$m(x) \mid b(x) - d(x).$$

Therefore

$$m(x) \mid (a(x) - c(x)) + (b(x) - d(x)) = (a(x) + b(x)) - (c(x) + d(x)).$$

So

$$a(x) + b(x) \equiv c(x) + d(x) \mod m(x),$$

which proves

$$[a(x) + b(x)] = [c(x) + d(x)].$$

Also,

$$\begin{aligned} a(x)b(x) - c(x)d(x) &= a(x)b(x) - c(x)b(x) + c(x)b(x) - c(x)d(x) \\ &= (a(x) - c(x))b(x) + c(x)(b(x) - d(x)). \end{aligned}$$

Since $m(x) \mid a(x) - c(x)$ and $m(x) \mid b(x) - d(x)$, it follows that

$$m(x) \mid a(x)b(x) - c(x)d(x).$$

So

$$a(x)b(x) \equiv c(x)d(x) \mod m(x),$$

which proves

$$[a(x)b(x)] = [c(x)d(x)].$$

□

Chapter 6

Ideals and Quotient Rings

6.1 Ideals and Quotient Rings

[6.1.0.1] Definition (*Quotient Rings*). Congruence classes mod $f(x)$ are denoted by $\mathbb{F}[x]/(f(x))$, and this is a ring. The additive identity of this ring is $[0] = [f(x)]$. This together is called a quotient ring, and it is closed under addition and multiplication.

[6.1.0.2] Theorem (*Class of $g(x)$*). $[g(x)] \in \mathbb{F}[x]/(f(x))$ is a unit if and only if

$$\gcd(f(x), g(x)) = 1.$$

That is, $g(x)$ and $f(x)$ are relatively prime.

$\therefore$

Proof. ($\Longleftarrow$). Suppose $\gcd(f(x), g(x)) = 1$. Then there exist $w(x), v(x) \in \mathbb{F}[x]$ such that

$$w(x)g(x) + v(x)f(x) = 1.$$

Thus

$$[w(x)g(x)] = [1],$$

so

$$[w(x)] = [g(x)]^{-1}.$$

($\Longrightarrow$). Suppose $[g(x)]$ is a unit. Then there exists $w(x) \in \mathbb{F}[x]$ such that

$$[w(x)g(x)] = [1].$$

So

$$w(x)g(x) \equiv 1 \mod f(x),$$

which means

$$f(x) \mid w(x)g(x) - 1.$$

Therefore there exists $v(x) \in \mathbb{F}[x]$ such that

$$w(x)g(x) - 1 = v(x)f(x),$$
$$w(x)g(x) - v(x)f(x) = 1.$$

Therefore,

$$\gcd(f(x), g(x)) = 1.$$

□

[6.1.0.3] Corollary. If $f(x)$ is irreducible in $\mathbb{F}[x]$, then $\mathbb{F}[x]/(f(x))$ is a field.

∴

Proof. If $g(x) \in \mathbb{F}[x]$ and $[g(x)] \neq [0]$, then $f(x) \nmid g(x)$. Since $f(x)$ is irreducible, this implies

$$\gcd(f(x), g(x)) = 1.$$

So by the previous theorem, $[g(x)]$ is a unit in $\mathbb{F}[x]/(f(x))$. Thus every nonzero element is a unit, and $\mathbb{F}[x]/(f(x))$ is a field. □

Let

$$\mathbb{E} = \mathbb{F}[x]/(f(x)).$$

Then we have an injection from $\mathbb{F} \to \mathbb{E}$ where $a \mapsto [a]$. So we may consider $\mathbb{F}$ as a subfield of $\mathbb{E}$.

[6.1.0.4] Definition (*Roots in Quotient Rings*). Suppose $\mathbb{F} \subseteq \mathbb{E}$. Let $\alpha = [x]$. Then for $f(x) \in \mathbb{E}[x]$, we have

$$f(\alpha) = [0].$$

[6.1.0.5] Axiom. $\mathbb{F} \cong \mathcal{E}$.

[6.1.0.6] Definition (*Ideal*). Let $\mathcal{R}$ be a commutative ring. Given that $I \subseteq \mathcal{R}$, we call I an ideal if and only if I is a subring of $\mathcal{R}$ and whenever $r \in \mathcal{R}$ and $a \in I$, then

$$ra \in I.$$

[6.1.0.7] Definition (*Congruence mod I*). Suppose $r, s \in \mathcal{R}$. We write

$$r \equiv s \mod I$$

if

$$r - s \in I.$$

[6.1.0.8] Theorem (*Congruence mod I is an Equivalence Relation*). Given $a, b, c \in \mathcal{R}$, congruence mod I is reflexive, symmetric, and transitive.

∴

Proof. **Reflexive.**

$$a \equiv a \mod I$$

because

$$a - a = 0 \in I.$$

Symmetric. If

$$a \equiv b \mod I,$$

then

$$a - b \in I.$$

Since I is a subring, $-(a-b) = b - a \in I$, so

$$b \equiv a \mod I.$$

Transitive. If

$$a \equiv b \mod I \quad \text{and} \quad b \equiv c \mod I,$$

then

$$a - b \in I \quad \text{and} \quad b - c \in I.$$

Since I is closed under addition,

$$(a-b) + (b-c) = a - c \in I.$$

Thus

$$a \equiv c \mod I.$$

□

[6.1.0.9] Definition (*Coset*). Instead of $[a]$ for $a \mod I$, we have the notation

$$a + I := \{a + i : i \in I\},$$

called a coset.

For example,

$$[a]_{\mathbb{Z}_m} = a + m\mathbb{Z}.$$

[6.1.0.10] Definition (*Quotient Ring*). $\mathcal{R}/I$ is called a quotient ring.

[6.1.0.11] Theorem (*Addition on Ideals*).

$$(a + I) + (b + I) = a + b + I$$

and

$$(a + I)(b + I) = ab + I.$$

∴

Proof. Suppose $a+I=c+I$ and $b+I=d+I$. Then

$$c-a\in I \quad \text{and} \quad d-b\in I.$$

Hence

$$(c-a)+(d-b)\in I,$$

which implies

$$(c+d)-(a+b)\in I.$$

Therefore

$$c+d+I=a+b+I.$$

To prove multiplication, since $c-a, d-b\in I$, we have

$$c(d-b)\in I \quad \text{and} \quad b(c-a)\in I$$

by the absorption property of ideals. Thus

$$c(d-b)+b(c-a)\in I.$$

But

$$c(d-b)+b(c-a)=cd-cb+bc-ba=cd-ab.$$

So

$$cd-ab\in I,$$

hence

$$ab+I=cd+I.$$

□

Quotient rings are independently associated with homomorphisms $\varphi:\mathcal{R}\to\mathcal{S}$.

[6.1.0.12] Definition (*Generators*). If $\mathcal{R}$ is any commutative ring and $a\in\mathcal{R}$, the ideal generated by a is

$$\{ra : r\in\mathcal{R}\} =: (a).$$

[6.1.0.13] Lemma. (a) is an ideal of $\mathcal{R}$.

∴

Proof. **Case 1.** If $r_1a, r_2a\in(a)$, then

$$r_1a+r_2a=(r_1+r_2)a\in(a).$$

Case 2. If $ra\in(a)$ and $s\in\mathcal{R}$, then

$$s(ra)=(sr)a\in(a).$$

□

These generators are called the principal ideal generated by a.

[6.1.0.14] Theorem. If $p(x)$ is irreducible in $\mathbb{F}[x]$, then the following are equivalent:

$$\mathbb{F}[x]/(p(x)) \text{ is a field} \iff \mathbb{F}[x]/(p(x)) \text{ is an integral domain.}$$

$\therefore$

Proof. We already know that if $p(x)$ is irreducible, then $\mathbb{F}[x]/(p(x))$ is a field. Every field is an integral domain, so one direction is immediate. Conversely, if $\mathbb{F}[x]/(p(x))$ is an integral domain, then $(p(x))$ is a prime ideal. In $\mathbb{F}[x]$, prime ideals generated by nonzero elements correspond to irreducible polynomials. Hence $p(x)$ is irreducible. □

Let $\mathcal{R}$ be a commutative ring with $1 \in \mathcal{R}$. Let A be any subset of $\mathcal{R}$. The ideal generated by A is the set of all finite linear combinations of elements of A:

$$(A) := \{r_1 a_1 + \ldots + r_n a_n : r_i \in \mathcal{R},\ a_i \in A\}.$$

Then (A) is the intersection of all ideals containing A. Suppose $\mathcal{R} = \mathbb{Z}$ and $a, b \in \mathbb{Z}$. Then the ideal generated by (a, b) is

$$(a, b) := \{xa + by : x, y \in \mathbb{Z}\}.$$

In fact,

$$(a, b) = \{r \cdot \gcd(a, b) : r \in \mathbb{Z}\}.$$

$\mathbb{Z}$ and $\mathbb{F}[x]$ are called principal ideal domains, while $\mathbb{Z}[x]$ and $\mathbb{Q}[x, y]$ are not principal ideal domains. Let

$$\varphi : \mathbb{Z} \to \mathbb{Z}/10\mathbb{Z},$$

defined by

$$\varphi(a) = [a]_{10} = a + 10\mathbb{Z}.$$

[6.1.0.15] Definition (*Kernel*). Let

$$K := \{x \in \mathbb{Z} : \varphi(x) = 0\}.$$

This is called the kernel of φ, written $\ker\varphi$.

[6.1.0.16] Theorem. K is an ideal in $\mathcal{R}$.

$\therefore$

Proof. **(1)** Suppose $x, y \in \ker\varphi$. Then

$$\varphi(x) = \varphi(y) = 0.$$

So

$$\varphi(x + y) = \varphi(x) + \varphi(y) = 0,$$

hence $x + y \in \ker\varphi$.

(2) Suppose $x \in \ker\varphi$ and $r \in \mathcal{R}$. Then

$$\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r) \cdot 0 = 0.$$

So $rx \in \ker\varphi$. Therefore $\ker\varphi$ is an ideal in $\mathcal{R}$. □

From the previous example,

$$\ker\varphi = (10) = 10\mathbb{Z}.$$

What we learned prior is that

$$\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}_{10}.$$

[6.1.0.17] Definition (*Image*).

$$\varphi := \{s \in \mathcal{S} : \exists r \in \mathcal{R},\ \varphi(r) = s\}.$$

[6.1.0.18] Theorem (*First Isomorphism Theorem*). Suppose $\varphi : \mathcal{R} \to \mathcal{S}$ is a homomorphism. Let $K = \ker\varphi$. Define

$$\overline{\varphi} : \mathcal{R}/K \to \varphi$$

by

$$\overline{\varphi}(r + K) = \varphi(r).$$

Then $\overline{\varphi}$ is an isomorphism from $\mathcal{R}/K$ to φ. So

$$\mathcal{R}/K \cong \varphi.$$

$\therefore$

Proof. □

[6.1.0.19] Proposition. Suppose $\varphi : \mathcal{R} \to \mathcal{S}$ is a ring homomorphism. Then φ is injective if and only if

$$\ker\varphi = \{0\}.$$

$\therefore$

Proof. ($\implies$). Suppose φ is injective. Let $r \in \ker\varphi$. So

$$\varphi(r) = 0.$$

But also

$$\varphi(0) = 0.$$

Since φ is injective, it follows that

$$r = 0.$$

Thus

$$\ker\varphi = \{0\}.$$

($\impliedby$). Suppose

$$\ker\varphi = \{0\}.$$

Let $r, s \in \mathcal{R}$ with

$$\varphi(r) = \varphi(s).$$

Then

$$\varphi(r) - \varphi(s) = 0,$$
$$\varphi(r - s) = 0.$$

So

$$r - s \in \ker\varphi.$$

Hence

$$r - s = 0,$$

therefore

$$r = s.$$

Thus φ is injective. □

[6.1.0.20] Theorem (*Proof of First Isomorphism Theorem*). Suppose $\varphi : \mathcal{R} \to \mathcal{S}$ is a homomorphism. Let $K = \ker\varphi$, and define

$$\overline{\varphi}(r + K) = \varphi(r).$$

Then $\overline{\varphi}$ is a well-defined isomorphism from $\mathcal{R}/K$ onto φ.

∴

Proof. To show $\overline{\varphi}$ is well-defined, suppose

$$r + K = s + K.$$

Then

$$r - s \in K = \ker\varphi,$$

so

$$\varphi(r - s) = 0.$$

Hence

$$\varphi(r) = \varphi(s).$$

Thus $\overline{\varphi}(r + K) = \overline{\varphi}(s + K)$. Now for $r, s \in \mathcal{R}$,

$$\overline{\varphi}((r + K) + (s + K)) = \overline{\varphi}(r + s + K) = \varphi(r + s) = \varphi(r) + \varphi(s) = \overline{\varphi}(r + K) + \overline{\varphi}(s + K),$$

and similarly,

$$\overline{\varphi}((r + K)(s + K)) = \overline{\varphi}(rs + K) = \varphi(rs) = \varphi(r)\varphi(s) = \overline{\varphi}(r + K)\overline{\varphi}(s + K).$$

So $\overline{\varphi}$ is a homomorphism. It is surjective by definition of φ. Indeed, if $s \in \varphi$, then there exists $r \in \mathcal{R}$ such that $\varphi(r) = s$. Hence

$$\overline{\varphi}(r + K) = s.$$

Its kernel is trivial. If

$$\overline{\varphi}(r + K) = 0,$$

then

$$\varphi(r) = 0,$$

so $r \in K$. Thus

$$r + K = K = 0 + K.$$

Therefore $\overline{\varphi}$ is injective. Hence $\overline{\varphi}$ is an isomorphism. □

[6.1.0.21] Example. Prove

$$\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}\left(\sqrt{2}\right).$$

Proof. Define

$$\varphi : \mathbb{Q}[x] \to \mathbb{C}$$

by

$$\varphi(f(x)) = f\left(\sqrt{2}\right).$$

Then

$$\ker\varphi := \{f(x) \in \mathbb{Q}[x] : f\left(\sqrt{2}\right) = 0\}.$$

Clearly,

$$x^2 - 2 \in \ker\varphi.$$

Claim.

$$\ker\varphi = (x^2-2).$$

Indeed, if $f\left(\sqrt{2}\right) = 0$, then by the factor theorem over $\mathbb{Q}\left(\sqrt{2}\right)$, $(x-\sqrt{2})$ divides $f(x)$. Since the coefficients of $f(x)$ are rational, $(x+\sqrt{2})$ also divides the conjugate relation, so

$$\left(x-\sqrt{2}\right)\left(x+\sqrt{2}\right) = x^2-2$$

divides $f(x)$ in $\mathbb{Q}[x]$. Thus every element of $\ker\varphi$ lies in (x^2-2), and the reverse inclusion is clear. Also,

$$\varphi = \mathbb{Q}\left(\sqrt{2}\right).$$

Therefore, by the first isomorphism theorem,

$$\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}\left(\sqrt{2}\right).$$

■

6.2 Field Extensions

[6.2.0.1] Definition (*Vector Space*). A vector space over $\mathbb{F}$ is an additive abelian group V equipped with scalar multiplication such that for $a, a_1, a_2 \in \mathbb{F}$ and $v, v_1, v_2 \in V$, the following hold:

1. $a(v_1+v_2) = av_1 + av_2$.
2. $(a_1+a_2)v = a_1v + a_2v$.

3. $a_1(a_2 v) = (a_1 a_2)v$.

4. $1_{\mathbb{F}} v = v$.

[6.2.0.2] Definition (*Span*). If every element of a vector space $V/\mathbb{F}$ can be written as a linear combination of elements of a set $\{v_1, v_2, \ldots, v_n\}$, then we say that $\{v_1, v_2, \ldots, v_n\}$ spans $V/\mathbb{F}$.

[6.2.0.3] Definition (*Linearly Independent*). A subset of a vector space $V/\mathbb{F}$ is linearly independent over $\mathbb{F}$ if whenever

$$c_1 v_1 + \cdots + c_n v_n = 0$$

with $c_i \in \mathbb{F}$, then $c_i = 0_{\mathbb{F}}$ for all i. Otherwise, it is dependent.

[6.2.0.4] Definition (*Basis*). A subset is called a basis if it is linearly independent and spans $V/\mathbb{F}$.

[6.2.0.5] Definition (*Dimension*). If $p(x) \in \mathbb{F}[x]$ is irreducible, then $\mathbb{E}$ is an extension field of $\mathbb{F}$. In fact, this is a vector space over $\mathbb{F}$. Its dimension is denoted by $[\mathbb{E} : \mathbb{F}]$.

[6.2.0.6] Theorem. Suppose K is an extension field of $\mathbb{E}$ and $\mathbb{E}$ is an extension field of $\mathbb{F}$. Then

$$[K : \mathbb{F}] = [K : \mathbb{E}][\mathbb{E} : \mathbb{F}].$$

∴

Proof. Suppose

$$[\mathbb{E} : \mathbb{F}] = n.$$

Let $v_1, \ldots, v_n \in \mathbb{E}$ be a basis for $\mathbb{E}/\mathbb{F}$. Suppose

$$[K : \mathbb{E}] = m.$$

Let $w_1, \ldots, w_m \in K$ be a basis for $K/\mathbb{E}$. Our claim is that

$$\{w_i v_j : 1 \le i \le m,\ 1 \le j \le n\}$$

is a basis for $K/\mathbb{F}$. First, we show that $\{w_i v_j\}$ spans K. Let $u \in K$. Since $\{w_i\}$ spans $K/\mathbb{E}$, we can write

$$u = \sum_{i=1}^{m} \alpha_i w_i, \qquad \alpha_i \in \mathbb{E}.$$

Since $\{v_j\}$ spans $\mathbb{E}/\mathbb{F}$, each α_i can be written as

$$\alpha_i = \sum_{j=1}^{n} \beta_{ij} v_j, \qquad \beta_{ij} \in \mathbb{F}.$$

Therefore

$$u = \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} w_i v_j.$$

So $\{w_i v_j\}$ spans $K/\mathbb{F}$. Now suppose

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} w_i v_j = 0, \qquad \beta_{ij} \in \mathbb{F}.$$

Rewrite this as

$$\sum_{i=1}^{m} \left(\sum_{j=1}^{n} \beta_{ij} v_j \right) w_i = 0.$$

Since the w_i are linearly independent over $\mathbb{E}$, we have

$$\sum_{j=1}^{n} \beta_{ij} v_j = 0$$

for each i. Since the v_j are linearly independent over $\mathbb{F}$, it follows that

$$\beta_{ij} = 0$$

for all i, j. Thus $\{w_i v_j\}$ is linearly independent over $\mathbb{F}$. Hence it is a basis of $K/\mathbb{F}$. Therefore

$$[K : \mathbb{F}] = mn = [K : \mathbb{E}][\mathbb{E} : \mathbb{F}].$$

□

[6.2.0.7] Definition (*Algebraic and Transcendental Functions*). Let $\mathbb{F} = q$, $\mathbb{E} = \mathbb{R}$, and $u = \pi$. There is no polynomial $p(u) = 0$ with $p(x) \in \mathbb{Q}[x]$. If there is no such polynomial, we say u is transcendental over $\mathbb{F}$. If there is such a polynomial, we say u is algebraic over $\mathbb{F}$.

To understand two versions of field extensions, let us look at when $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$. We can use the first isomorphism theorem.

[6.2.0.8] Lemma ($\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$). For the evaluation map $\varphi : \mathbb{Q}[x] \to \mathbb{Q}[\alpha]$, we have

$$\begin{aligned} \varphi \text{ is injective} &\iff \ker \varphi = \{0\} \\ &\iff \nexists f(x) \in \mathbb{Q}[x] \text{ such that } f(\alpha) = 0 \\ &\iff \alpha \text{ is transcendental over } \mathbb{Q}. \end{aligned}$$

∴

Proof. □

Proof. Using the first isomorphism theorem, let φ be the homomorphism defined by evaluation at α. Then

$$\varphi = \{f(\alpha) : f(x) \in \mathbb{Q}[x]\} = \mathbb{Q}[\alpha].$$

So φ is surjective. Also,

$$\ker\varphi = \{f(x) \in \mathbb{Q}[x] : f(\alpha) = 0\}.$$

Thus φ is injective if and only if $\ker\varphi = \{0\}$, which happens if and only if there is no nonzero polynomial in $\mathbb{Q}[x]$ with α as a root. That is exactly the statement that α is transcendental over q. Therefore, if α is transcendental over q, then

$$\mathbb{Q}[\alpha] \cong \mathbb{Q}[x].$$

So $\mathbb{Q}[\alpha]$ is a ring, not a field. ■

[6.2.0.9] Definition (*Minimal Polynomial*). Suppose $p(x)$ is a monic polynomial of smallest degree such that

$$p(\alpha) = 0.$$

This is called the minimal polynomial of α/q.

[6.2.0.10] Lemma. The minimal polynomial $p(x)$ is irreducible.

$\therefore$

Proof. Suppose $p(x)$ is reducible. Then

$$p(x) = q(x)g(x)$$

for some nonconstant $q(x), g(x) \in \mathbb{Q}[x]$. Evaluating at α gives

$$0 = p(\alpha) = q(\alpha)g(\alpha).$$

So either $q(\alpha) = 0$ or $g(\alpha) = 0$. But then either $q(x)$ or $g(x)$ is a polynomial of smaller degree than $p(x)$ having α as a root. This contradicts the minimality of $p(x)$. Therefore $p(x)$ is irreducible. □

Proof. Using the first isomorphism theorem, suppose α is algebraic. Let

$$\varphi : \mathbb{Q}[x] \to \mathbb{Q}[\alpha]$$

be evaluation at α. Then

$$\ker\varphi = (p(x)),$$

where $p(x)$ is the irreducible minimal polynomial of α. Therefore

$$\mathbb{Q}[x]/(p(x)) \cong \mathbb{Q}[\alpha].$$

Since $p(x)$ is irreducible, $\mathbb{Q}[x]/(p(x))$ is a field. So $\mathbb{Q}[\alpha]$ is a field. Hence

$$\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha).$$

■

We have previously learned that $\mathbb{Q}(r)$ is a vector space.

$$\mathbb{Q}(r) = \mathbb{Q}[r]$$

What is the dimension $[\mathbb{Q}[r]:\mathbb{Q}]$. We have to find the basis. So what is the basis of $\mathbb{Q}[r]/q$.

[6.2.0.11] Lemma. A basis is

$$1, r, r^2, \ldots, r^{n-1},$$

where $n = \deg f(x)$ and $f(x)$ is the minimal polynomial of r/q.

∴

Proof. □

Proof. Since

$$\mathbb{Q}[r] = \{g(r) : g(x) \in \mathbb{Q}[x]\},$$

every element of $\mathbb{Q}[r]$ is obtained by evaluating a polynomial at r. Let $f(x)$ be the minimal polynomial of r, with $\deg f(x) = n$ and $f(r) = 0$. Take any $g(x) \in \mathbb{Q}[x]$. By the division algorithm,

$$g(x) = f(x)q(x) + s(x),$$

where $\deg s(x) < \deg f(x) = n$. Plug in r:

$$g(r) = f(r)q(r) + s(r) = s(r),$$

since $f(r) = 0$. Thus $g(r)$ is a linear combination of

$$1, r, r^2, \ldots, r^{n-1}.$$

So these elements span $\mathbb{Q}[r]$. To see they are linearly independent, suppose

$$c_0 + c_1 r + \cdots + c_{n-1} r^{n-1} = 0$$

with $c_i \in \mathbb{Q}$. Then the polynomial

$$c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

has r as a root, but its degree is less than n. This contradicts the minimality of $f(x)$ unless all $c_i = 0$. Therefore

$$1, r, r^2, \ldots, r^{n-1}$$

is a basis. ■

[6.2.0.12] Definition (*Adjoin*). We say that $\mathbb{F}(u)$ is a field made by adjoining u to $\mathbb{F}$.

[6.2.0.13] Theorem. Let $\mathbb{K}/\mathbb{F}$ and let $u \in \mathbb{K}$ be an algebraic element over $\mathbb{F}$ with minimal polynomial $p(x)$ of degree n. Then

1. $\mathbb{F}(u) \cong \mathbb{F}[x]/(p(x))$;
2. $\{1_{\mathbb{F}}, u, u^2, \ldots, u^{n-1}\}$ is a basis of the vector space $\mathbb{F}(u)$ over $\mathbb{F}$;
3. $[\mathbb{F}(u):\mathbb{F}] = n$.

∴

Proof. □

[6.2.0.14] Corollary. If u and v have the same minimal polynomial $p(x)$ in $\mathbb{F}[x]$, then

$$\mathbb{F}(u) \cong \mathbb{F}(v).$$

$\therefore$

Proof. □

[6.2.0.15] Definition (*Algebraic Extension*). An extension field $\mathbb{K}$ of a field $\mathbb{F}$ is said to be an algebraic extension if every element of $\mathbb{K}$ is algebraic over $\mathbb{F}$.

[6.2.0.16] Theorem. If $\mathbb{K}$ is a finite-dimensional extension field of $\mathbb{F}$, then $\mathbb{K}$ is an algebraic extension of $\mathbb{F}$.

$\therefore$

Proof. Let $u \in \mathbb{K}$. Since $\mathbb{K}$ is finite-dimensional over $\mathbb{F}$, the set

$$\{1, u, u^2, \ldots, u^n\}$$

must be linearly dependent over $\mathbb{F}$ for n large enough. So there exist $a_0, \ldots, a_n \in \mathbb{F}$, not all zero, such that

$$a_0 + a_1 u + \cdots + a_n u^n = 0.$$

Thus u satisfies a nonzero polynomial with coefficients in $\mathbb{F}$. So u is algebraic over $\mathbb{F}$. Since u was arbitrary, every element of $\mathbb{K}$ is algebraic over $\mathbb{F}$. Hence $\mathbb{K}$ is an algebraic extension of $\mathbb{F}$. □

Chapter 7

Geometric Constructions

7.1 Constructible Shapes

Which regular n-gons can be constructed?

[7.1.0.1] Definition (*Constructible*). a is constructible if you can construct a line segment of length a.

[7.1.0.2] Definition (*Constructible Point*). A point in $\mathbb{R}^2$ is constructible if its coordinates are constructible.

[7.1.0.3] Definition (*Constructible Line*). A constructible line is a line determined by constructible points.

[7.1.0.4] Theorem. Constructible numbers lie in field extensions of q.

$\therefore$

Proof. Suppose a, b are constructible. Then they are closed under addition, subtraction, multiplication, and division by nonzero elements. Hence constructible numbers lie in a field extension of q. □

[7.1.0.5] Theorem. If a is constructible and $a \geq 0$, then $\sqrt{a}$ is constructible.

$\therefore$

Proof. Suppose a triangle is enclosed in a semicircle with triangle side length 1 and diameter $\frac{a+1}{2}$. The relevant distance x satisfies

$$x^2 = \left(\frac{a+1}{2}\right)^2 - \left(\frac{a-1}{2}\right)^2.$$

Thus

$$x^2 = a.$$

So the distance $x = \sqrt{a}$ is constructible. □

Suppose we have constructible points. How do we get new points by intersecting lines, circles, and lines with circles?

[7.1.0.6] Definition (*New Constructible Points*). If α is obtained from a constructible configuration, then adjoining α gives a quadratic extension. That is, any constructible point lies in a tower of fields

$$\mathbb{Q} \subseteq \mathbb{Q}[a_1] \subseteq \mathbb{Q}[a_1, a_2] \subseteq \ldots \subseteq \mathbb{F},$$

where

$$\mathbb{F}_k = \mathbb{F}_{k-1}[a_k]$$

and

$$[\mathbb{F}_k : \mathbb{F}_{k-1}] = 2.$$

Let α be the root of a quadratic polynomial. So every constructible number lies in a field $\mathbb{F}$ where

$$[\mathbb{F} : \mathbb{Q}] = 2^n$$

for some n. Therefore $\sqrt[3]{2}$ is not constructible.

[7.1.0.7] Lemma (*Constructible Points*). Let $r \in \mathbb{R}$. Then r is constructible with straightedge and compass if and only if r lies in a field extension $\mathbb{E}$ with

$$[\mathbb{E} : \mathbb{Q}] = 2^n$$

for some n.

∴

Proof. □

π is not constructible, and neither is it algebraic. Therefore constructible points are only possible if

$$[\mathbb{Q}(r) : \mathbb{Q}] = 2^k$$

for some k. We will show that we cannot trisect 60°, since we can construct 60°, implying that not every angle can be trisected. Because $20° = \theta = \frac{\pi}{9}$ would need to be constructible, the number $\cos\theta$ would need to be constructible.

$$\begin{aligned}\cos 2\theta &= \cos^2\theta - \sin^2\theta \\ &= 2\cos^2\theta - 1,\end{aligned}$$

and

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

If $\theta = \dfrac{\pi}{9}$, then

$$\cos 3\theta = \cos\frac{\pi}{3} = \frac{1}{2}.$$

Let $x = \cos 20°$. Then

$$\frac{1}{2} = 4x^3 - 3x,$$
$$0 = 8x^3 - 6x - 1.$$

We claim that $8x^3 - 6x - 1$ is irreducible over $\mathbb{Q}$. By the rational root test, the only possible rational roots are

$$\pm 1,\ \pm\frac{1}{2},\ \pm\frac{1}{4},\ \pm\frac{1}{8},$$

and none of these are roots. So the polynomial is irreducible over $\mathbb{Q}$. Hence

$$[\mathbb{Q}(x) : \mathbb{Q}] = 3,$$

which is not a power of 2. Therefore $x = \cos 20°$ is not constructible, so $60°$ cannot be trisected.

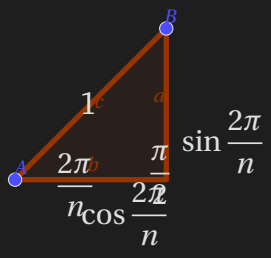
Question: Which regular n-gons can be constructed? That is, for which n can the angle

$$\frac{2\pi}{n}$$

be constructed. Such an angle can be constructed if and only if

$$\cos\frac{2\pi}{n} \quad \text{and} \quad \sin\frac{2\pi}{n}$$

can be constructed.



Thus a regular n-gon is constructible if and only if

$$\left(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n}\right)$$

is a constructible point. If we let

$$\rho = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n},$$

then

$$\rho^n = 1.$$

So ρ is an nth root of unity satisfying

$$x^n - 1 = 0.$$

Suppose

$$n = 2^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

is a prime factorization, where $p_1 = 2$ and p_j is odd for $j \geq 2$. Then the regular n-gon is constructible if and only if each odd prime factor occurs to the first power and each such odd prime is a Fermat prime.

[7.1.0.8] Definition (*Fermat Prime*). If

$$2^{2^k} + 1 = p$$

is prime, then p is a Fermat prime.

[7.1.0.9] Corollary. The constructible regular n-gons are exactly those for which

$$n = 2^m p_1 p_2 \cdots p_r,$$

where the p_i are distinct Fermat primes.

$\therefore$

Proof. □

[7.1.0.10] Proposition. Let $\varphi : \mathbb{Q}[x] \to \mathbb{Q}[\alpha]$ be defined by

$$\varphi(p(x)) = p(\alpha).$$

Then φ is surjective.

$\therefore$

Proof. Suppose $\beta \in \mathbb{Q}[\alpha]$. Then by definition of $\mathbb{Q}[\alpha]$, there exists $f(x) \in \mathbb{Q}[x]$ such that

$$\beta = f(\alpha).$$

Thus

$$\varphi(f(x)) = f(\alpha) = \beta.$$

So φ is surjective. □

φ is injective if and only if $\ker \varphi = \{0\}$. This is a consequence of the first isomorphism theorem.

[7.1.0.11] Proposition.

$$\ker \varphi = \{0\} \iff (\forall f(x) \in \mathbb{Q}[x],\ f(\alpha) = 0 \Rightarrow f(x) = 0) \iff \alpha/\mathbb{Q} \text{ is transcendental.}$$

$\therefore$

Proof. □

Chapter 8

Groups

8.1 Definition of Groups

A group is a one-operation analogue of a ring. Groups are often thought of as bijections from a set to itself, or permutations. Most of the course we will be looking at finite groups.

Let X be a set. Assume $X \neq \varnothing$. Let S_X, called the symmetric group on X, be the set of permutations of X, equivalently the bijections $X \to X$.

Composition has the following properties. There is an identity permutation, denoted by e, i, or 1. Composition is associative:

$$(a \circ b) \circ c = a \circ (b \circ c).$$

Every element has a unique inverse, since each permutation is a bijection. If f is a permutation of X, then its unique inverse is denoted by f^{-1}.

An abstract group G is a nonempty set with a binary operation, usually denoted by $\cdot$, $*$, or juxtaposition. There is an identity element, say 1, such that

$$1 * a = a * 1 = a$$

for all $a \in G$. A group does not need to be commutative, though the identity commutes with every element. The operation is associative, so for all $a, b, c \in G$,

$$(a * b) * c = a * (b * c) = a * b * c.$$

Every element $a \in G$ has an inverse a^{-1}.

[8.1.0.1] Definition (*Abelian Groups*). A group G does not need to be commutative, but if it is, we call it a commutative group, or **abelian**.

S_X is the group of permutations on X under composition. If G is a subset of S_X which is closed under composition and inverses, then G is a group. Cayley's Theorem says that every group is isomorphic to a subgroup of some symmetric group. We will prove this later.

Suppose

$$X := \{1, 2, \ldots, n\}.$$

Then S_X is denoted by S_n, the symmetric group on n letters. For example, S_3 is the set of permutations of $\{1,2,3\}$. The notation for permutations is as follows. Suppose $\sigma \in S_3$. Then we denote it by

$$\begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix}.$$

The elements of S_3 are

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$
$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Suppose $\sigma_2 \circ \sigma_4$. Then we follow elements through σ_4 first and then σ_2. Doing this gives

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

[8.1.0.2] Example.

$$\sigma_4 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

If $(\mathcal{R}, +, \cdot)$ is a ring with operations addition and multiplication, then $(\mathcal{R}, +)$ is a group. The identity in an additive group is 0. It is associative, and every element a has an additive inverse, denoted by $-a$. In fact, these groups are abelian. Let $\mathbb{F}$ be any field. Let

$$\mathbb{F}^* := \{a \in \mathbb{F} : a \neq 0\} := U(\mathbb{F}).$$

Then $\mathbb{F}^*$ is a group under multiplication. This group has identity $1 \in \mathbb{F}$, it is associative, and every element has an inverse. More generally, if $\mathcal{R}$ is a ring, then

$$\mathcal{R}^* := \{a \in \mathcal{R} : a \text{ is a unit in } \mathcal{R}\} := U(\mathcal{R})$$

is a group.

[8.1.0.3] Example.

$$\mathbb{Z}_6^* = \{1, 5\}.$$

8.2 Properties of Groups

[8.2.0.1] Definition (*Group under Multiplication*). Suppose G is a group $(G, *)$, where

$$* : G \times G \to G.$$

Then:

$$1 \in G,$$
$$1 * a = a * 1 \quad \forall a \in G,$$
$$(a * b) * c = a * (b * c) \quad \forall a, b, c \in G,$$
$$\forall a \in G,\ \exists a^{-1} \in G \text{ such that } a^{-1} * a = aa^{-1} = 1.$$

Also,

$$a^2 = a * a,$$

and inductively,

$$a^n = a(a^{n-1}) = a * a * \cdots * a.$$

S_X is the group of permutations on X under composition, and it is noncommutative for $\#X \geq 3$. If $(\mathcal{R}, +, *)$ is a ring, then $(\mathcal{R}, +)$ is a group under addition, and it is commutative. Note that $(\mathcal{R}, +, *)$ is ring notation, not group notation. This means that $0 \in \mathcal{R}$ is allowed even though multiplication is closed, because we are not saying $(\mathcal{R}, *)$ is a group.

Also,

$$U(\mathcal{R}) = \mathcal{R}^* = \{u \in \mathcal{R} : \exists v \in \mathcal{R} \text{ with } uv = vu = 1\}$$

is a group.

[8.2.0.2] Example.

$$\mathbb{Z}_m^*$$

is the group of units in $\mathbb{Z}_m$. For example,

$$\mathbb{Z}_6^* = \{1, 5\},$$
$$\mathbb{Z}_8^* = \{1, 3, 5, 7\},$$
$$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}.$$

If $\mathcal{R}$ is any ring, then

$$\mathbf{Mat}n(\mathcal{R})$$

is the ring of $n \times n$ matrices with entries in $\mathcal{R}$. Also,

$$\mathbf{Mat}n(\mathcal{R})^*$$

is the group of invertible matrices with entries in $\mathcal{R}$. If $n \geq 2$, then $\mathbf{Mat}n(\mathcal{R})^*$ is nonabelian. If $\mathbb{F}$ is a field, then matrices represent transformations of vector spaces. $\mathbf{Mat}n(\mathbb{F})$ corresponds to linear transformations of an n-dimensional vector space over $\mathbb{F}$.

Suppose $A \in \mathbf{Mat}n(\mathbb{F})$, and V is an n-dimensional vector space. We define

$$T(v) = Av,$$

so $T : V \to V$ is a linear transformation. Then

$$T(\lambda v + \mu w) = \lambda T(v) + \mu T(w).$$

[8.2.0.3] Definition (*General Linear Group*). The group of invertible $n \times n$ matrices with entries in $\mathbb{F}$ under multiplication is denoted by

$$GL_n(\mathbb{F}).$$

This is called the General Linear Group.

[8.2.0.4] Example. $GL_2(\mathbb{F}_2)$ consists of matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $a, b, c, d \in \{0, 1\}$, and such a matrix is invertible if and only if

$$ad - bc \neq 0.$$

The invertible matrices are

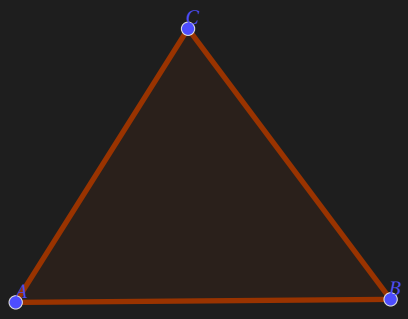
$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

So

$$\#GL_2(\mathbb{F}_2) = 6,$$

which is isomorphic to S_3.

Coming from geometry, we also get groups. If you take a solid or a regular n-gon and consider its rigid motions, then these form a group. A rigid motion is a motion that picks up the figure and puts it back in place, such as a rotation or reflection.



[8.2.0.5] Example. Rigid motions of a regular 3-gon are: the identity, rotation by $120° = \frac{2\pi}{3}$ counterclockwise, call this r, rotation by $240° = \frac{4\pi}{3}$, call this r^2, and reflections.

$$1 : 1 \to 1,\ 2 \to 2,\ 3 \to 3$$
$$r : 1 \to 2 \to 3 \to 1$$
$$r^2 : 1 \to 3 \to 2 \to 1$$
$$s : 1 \to 1,\ 2 \leftrightarrow 3$$
$$sr : 1 \leftrightarrow 3,\ 2 \to 2$$
$$rs : \text{reflection through vertex } 3.$$

This group is denoted D_3. It has order 6 and is called the dihedral group. Some texts use D_6. Others use D_n or D_{2n} depending on convention.

[8.2.0.6] Example. Let H, K be groups. Then $H \times K$ has underlying set $H \times K$ with operation

$$(h_1, k_1) * (h_2, k_2) = (h_1 * h_2, k_1 * k_2).$$

This makes $H \times K$ into a group. The identity is $(1, 1)$. Associativity holds componentwise. The inverse is

$$(h, k)^{-1} = (h^{-1}, k^{-1}).$$

Closure also holds componentwise.

$(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ has order 4. $(\mathbb{Z}_4, +)$ also has 4 elements. $\mathbb{Z}_5^*$ and $\mathbb{Z}_8^*$ also have 4 elements. Now, are they isomorphic. Let us look at the tables for these groups.

$(\mathbb{Z}_4, +)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_5^*$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

A possible isomorphism is

$$0 \mapsto 1,$$
$$1 \mapsto 2,$$

$$2 \mapsto 4,$$
$$3 \mapsto 3.$$

[8.2.0.7] THEOREM (*Fundamental Theorem of Finite Abelian Groups*). Every finite abelian group is a direct product of groups of the form $(\mathbb{Z}_n, +)$ for various n.

$\therefore$

Proof. □

[8.2.0.8] DEFINITION (*Other Properties of Groups*). Let G be a group. Some other properties which follow from the definition are the following.

1. Cancellation law. Suppose $a, b, c \in G$. If
$$ba = ca,$$
then
$$b = c.$$
2. Identity is unique.
3. Inverses are unique.
4. $$(ab)^{-1} = b^{-1}a^{-1}.$$
5. $$(a^{-1})^{-1} = a.$$

[8.2.0.9] PROPOSITION. The cancellation law holds in any group.

$\therefore$

Proof. Suppose
$$ab = ac.$$
Then
$$a^{-1}(ab) = a^{-1}(ac),$$
$$(a^{-1}a)b = (a^{-1}a)c,$$
$$1b = 1c,$$
$$b = c.$$
A similar argument proves right cancellation. □

[8.2.0.10] PROPOSITION. The identity element in a group is unique.

$\therefore$

Proof. Suppose e and f are both identities. Then

$$ef = f$$

since e is an identity, and

$$ef = e$$

since f is an identity. Thus

$$e = f.$$

□

[8.2.0.11] Proposition. Inverses in a group are unique.

∴

Proof. Suppose $a \in G$, and $b, c \in G$ both satisfy

$$ba = ab = e \quad \text{and} \quad ca = ac = e.$$

Then

$$b = be = b(ac) = (ba)c = ec = c.$$

Thus $b = c$. □

[8.2.0.12] Proposition. For all $a, b \in G$,

$$(ab)^{-1} = b^{-1}a^{-1}.$$

∴

Proof. We compute

$$(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e,$$

and similarly

$$(b^{-1}a^{-1})(ab) = e.$$

By uniqueness of inverse,

$$(ab)^{-1} = b^{-1}a^{-1}.$$

□

[8.2.0.13] Proposition. For all $a \in G$,

$$(a^{-1})^{-1} = a.$$

∴

Proof. Since

$$a^{-1}a = aa^{-1} = e,$$

a is an inverse of a^{-1}. By uniqueness of inverse,

$$(a^{-1})^{-1} = a.$$

□

[8.2.0.14] Definition (*Order*). Let G be a group and let $a \in G$. The order of a is the smallest strictly positive integer n such that

$$a^n := a * a * \cdots * a = 1.$$

If there is no such n, then a has infinite order.

[8.2.0.15] Theorem. If $\#G$ is finite, then every $a \in G$ has finite order.

∴

Proof. Since G is finite, the list

$$1, a, a^2, a^3, \ldots$$

cannot consist of distinct elements forever. So there exist integers $i < j$ such that

$$a^i = a^j.$$

By cancellation,

$$1 = a^{j-i}.$$

Thus a has finite order. □

[8.2.0.16] Example. Dihedral groups have finite order for all elements.

[8.2.0.17] Example ($G_1 = (\mathbb{Z}_4, +)$).

Elements	Order
0	1
1	4
2	2
3	4

[8.2.0.18] Example ($G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$).

Elements	Order
(0,0)	1
(0,1)	2
(1,0)	2
(1,1)	2

[8.2.0.19] Example ($G_3 = \mathbb{Z}_5^*$).

Elements	Order
1	1
2	4
3	4
4	2

This is another way of showing that G_1 and G_3 are isomorphic.

[8.2.0.20] Corollary (*Infinite Order*). Suppose $a^n \neq e$ for all $n > 0$. Then $|a| = \infty$.

$\therefore$

Proof. □

[8.2.0.21] Theorem. Suppose $a \in G$ and $|a| = n$. If $k \in \mathbb{Z}$, then

$$a^k = 1 \quad \text{if and only if} \quad n \mid k.$$

$\therefore$

Proof. ($\Longrightarrow$). Suppose $k \in \mathbb{Z}$ such that $a^k = 1$. Write

$$k = nq + r$$

with $0 \leq r < n$. Then

$$\begin{aligned} a^k &= a^{nq+r} \\ &= a^{nq} a^r \\ &= (a^n)^q a^r \\ &= 1^q a^r \\ &= a^r. \end{aligned}$$

Since $a^k = 1$, we get $a^r = 1$. But n is the smallest positive integer with this property, so $r = 0$. Thus $n \mid k$.

($\Longleftarrow$). If $n \mid k$, then $k = nq$ for some q. Thus

$$\begin{aligned} a^k &= a^{nq} \\ &= (a^n)^q \\ &= 1^q \\ &= 1. \end{aligned}$$

So $a^k = 1$. □

[8.2.0.22] Corollary.

$$a^i = a^j \quad \text{if and only if} \quad a^{i-j} = 1.$$

Thus

$$n \mid i - j$$

or equivalently

$$i \equiv j \mod n.$$

Proof. ($\Longrightarrow$). Given $a^i = a^j$, then

$$a^i a^{-j} = a^j a^{-j},$$
$$a^{i-j} = 1.$$

($\Longleftarrow$). Given $a^{i-j} = 1$, then

$$a^i a^{-j} = 1,$$
$$a^i = a^j.$$

□

[8.2.0.23] THEOREM. Suppose $|a| = n$ and $t \mid n$. Then

$$|a^t| = \frac{n}{t}.$$

Proof. Let $|a^t| = k$. Since $a^n = 1$, we have

$$(a^t)^{n/t} = a^n = 1,$$

so

$$k \mid \frac{n}{t}.$$

Also, since $(a^t)^k = 1$, we have

$$a^{tk} = 1.$$

Thus

$$n \mid tk.$$

Since $t \mid n$, it follows that

$$\frac{n}{t} \mid k.$$

Therefore

$$k = \frac{n}{t}.$$

□

Suppose $|a| = 6$, then

$$|a^4| = 3.$$

More generally, for $t \in \mathbb{Z}$ with $t > 0$, we have

$$|a^t| = \frac{n}{\gcd(t,n)}.$$

[8.2.0.24] Proposition. If $|a| = n$ and $d = \gcd(t,n)$, then

$$|a^t| = \frac{n}{d}.$$

Proof. Let $|a^t| = k$. We know $a^n = 1$. Then

$$(a^t)^{n/d} = a^{tn/d} = \left(a^n\right)^{t/d} = 1,$$

since $t/d \in \mathbb{Z}$. So

$$k \mid \frac{n}{d}.$$

Also, since $(a^t)^k = 1$, we have

$$a^{tk} = 1,$$

so

$$n \mid tk.$$

Dividing by d gives

$$\frac{n}{d} \mid k \cdot \frac{t}{d}.$$

Because $\gcd(n/d, t/d) = 1$, it follows that

$$\frac{n}{d} \mid k.$$

Thus

$$k = \frac{n}{d}.$$

□

8.3 Subgroups

[8.3.0.1] Definition (*Subgroup*). Let G be a group and let $\varnothing \neq H \subseteq G$. We say H is a subgroup of G if H is a group under the operation of G. That is, for all $a, b \in H$, we have $ab \in H$, $1 \in H$, and if $a \in H$, then $a^{-1} \in H$. Associativity is inherited from G. This is denoted by

$$H \leq G.$$

Something to note that you may realize through a lot of practice problems is that

$$H \leq G$$

if and only if for all $a, b \in H$,

$$ab^{-1} \in H.$$

We could also have a subgroup $H \leq G$ with $\text{ord}(H) < \infty$. Then $H \leq G$ if and only if $H \neq \varnothing$ and H is closed under the operation of the group.

[8.3.0.2] Example. Let H be a finite nonempty subset of a group G that is closed under the group operation. Then H is a subgroup of G. Indeed, let $a \in H$. Since H is finite, the sequence

$$a, a^2, a^3, \ldots$$

must repeat, so $a^m = a^n$ for some $m > n$. Then

$$a^{m-n} = 1.$$

Hence

$$a^{-1} = a^{m-n-1} \in H.$$

So every element of H has an inverse in H, and therefore $H \leq G$.

$G = GL(n, \mathbb{F})$ is the group of nonsingular $n \times n$ matrices with entries in $\mathbb{F}$. This is called the General Linear Group. One of our exercises is that

$$SL(n, \mathbb{F})$$

is the set of matrices in $GL(n, \mathbb{F})$ with determinant 1. This is called the Special Linear Group. Since

$$\det(AB) = \det(A)\det(B),$$

if $\det(A) = \det(B) = 1$, then

$$\det(AB) = 1.$$

Also, if $\det(A) = 1$, then

$$\det\left(A^{-1}\right) = \frac{1}{\det(A)} = 1.$$

So $SL(n, \mathbb{F}) \leq GL(n, \mathbb{F})$. Let $\mathbb{C}^*$ be the set of nonzero complex numbers. Let $n \in \mathbb{Z}^{>0}$. Then

$$\left\{\exp\left(\frac{2k\pi i}{n}\right) : k = 0, \ldots, n-1\right\}$$

is the set of complex nth roots of unity. Also,

$$\exp\left(\frac{2k\pi i}{n}\right) = \cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right).$$

We can think of multiplication here as cyclical. Given any group, there are important examples you can get from any group.

[8.3.0.3] Definition (*Cyclic Subgroup Generated by a*). Let $a \in G$. The cyclic subgroup generated by a, denoted by $\langle a \rangle$, is

$$\langle a \rangle := \{a^n : n \in \mathbb{Z}\}.$$

We need $n \in \mathbb{Z}$ since we want all powers, positive and negative, because the order can be finite or infinite. Since it is closed under multiplication and inverses, it is also a subgroup. We consider this as the smallest subgroup of G containing a. We call this cyclic because when the order is finite,

the powers repeat in a cycle. For an infinite subgroup, look at $(\mathbb{Z}, +)$. The subgroup generated by 2 is

$$\ldots, -4, -2, 0, 2, 4, \ldots.$$

For example, if $H \leq G$ and $a \in H$, then

$$\langle a \rangle \leq H.$$

[8.3.0.4] Definition (*Subgroup Generated by a Subset*). If $S \subseteq G$, the subgroup generated by S, denoted by $\langle S \rangle$, is the smallest subgroup of G containing S. This is the same as

$$\bigcap_{H \leq G \text{ and } S \subseteq H} H,$$

which is the intersection of all subgroups of G containing S.

For example, if we take two appropriate elements of a symmetric group, they may generate the entire group. Similar to ideals, we also have trivial subgroups. For example, ponder looking at the subgroup generated by the identity element.

[8.3.0.5] Definition. If G is a group and

$$G = \langle a \rangle$$

for some $a \in G$, then G is cyclic.

$(\mathbb{Z}_n, +)$ is cyclic, since it is generated by 1. It is also generated by any $m \in \mathbb{Z}_n$ such that

$$\gcd(m, n) = 1.$$

Also,

$$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$$

is cyclic, generated by 2 or 3. For

$$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\},$$

we note that

$$2^3 = 8 \equiv 1 \mod 7,$$

so 2 does not generate the whole group. However,

$$3^2 = 9 \equiv 2 \mod 7,$$

and since $2^3 \equiv 1 \mod 7$, we get

$$3^6 \equiv 1 \mod 7.$$

In fact, the powers of 3 run through all nonzero classes mod 7, so $\text{ord}(3) = 6$. Since

$$\text{ord}(\mathbb{Z}_7^*) = 6,$$

the group is cyclic.

[8.3.0.6] Theorem. If p is prime, then $\mathbb{Z}_p^*$ is cyclic.

$\therefore$

Proof. This is a standard theorem in group theory and number theory. The proof is more extensive than what we need right now, but the result is important to know. □

8.4 Group Homomorphisms and Isomorphisms

[8.4.0.1] Definition (*Group Homomorphism*). If we let $f : G \to H$ be a function between groups, then f is a homomorphism if for all $a, b \in G$,

$$f(ab) = f(a)f(b).$$

[8.4.0.2] Definition (*Group Isomorphism*). A map $f : G \to H$ is an isomorphism if it is a bijective homomorphism.

[8.4.0.3] Example. Let

$$G := \left\{ \exp\left(\frac{2k\pi i}{n}\right) : k = 0, \ldots, n-1 \right\}$$

under multiplication. Let

$$H := (\mathbb{Z}_n, +).$$

Define

$$f : G \to H$$

by

$$f\left(\exp\left(\frac{2k\pi i}{n}\right)\right) = k \in \mathbb{Z}_n.$$

Prove that G and H are isomorphic.

[8.4.0.4] Proposition. The map

$$f\left(\exp\left(\frac{2k\pi i}{n}\right)\right) = k$$

defines an isomorphism

$$G \cong \mathbb{Z}_n.$$

$\therefore$

Proof. First, f is a homomorphism. If

$$\exp\left(\frac{2k\pi i}{n}\right), \exp\left(\frac{2\ell\pi i}{n}\right) \in G,$$

then

$$\begin{aligned} f\left(\exp\left(\frac{2k\pi i}{n}\right)\exp\left(\frac{2\ell\pi i}{n}\right)\right) &= f\left(\exp\left(\frac{2(k+\ell)\pi i}{n}\right)\right) \\ &= k + \ell \\ &= f\left(\exp\left(\frac{2k\pi i}{n}\right)\right) + f\left(\exp\left(\frac{2\ell\pi i}{n}\right)\right). \end{aligned}$$

So f is a homomorphism. To check injectivity, note that

$$\exp\left(\frac{2k\pi i}{n}\right) = \exp\left(\frac{2\ell\pi i}{n}\right)$$

if and only if

$$\exp\left(\frac{2(k-\ell)\pi i}{n}\right) = 1,$$

if and only if

$$\frac{2(k-\ell)\pi}{n}$$

is a multiple of 2π, if and only if

$$n \mid (k-\ell),$$

if and only if

$$k \equiv \ell \mod n.$$

Thus f is well-defined and injective. It is surjective because every class $k \in \mathbb{Z}_n$ is hit by

$$\exp\left(\frac{2k\pi i}{n}\right).$$

Hence f is an isomorphism. □

[8.4.0.5] Example. The map

$$f : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$$

defined by

$$f(k) = [k]$$

is a homomorphism because

$$[k+\ell] = [k] + [\ell].$$

It is not injective because

$$f(0) = f(n) = f(2n).$$

But it is surjective, since every class in $\mathbb{Z}_n$ is of the form $[k]$.

[8.4.0.6] Example. Let

$$G := \left\{\exp\left(\frac{2\pi ki}{n}\right) : k \in \mathbb{Z}\right\}.$$

Then

$$f : (\mathbb{Z}, +) \to G$$

defined by

$$f(k) = \exp\left(\frac{2\pi ki}{n}\right)$$

is a homomorphism since

$$f(k+\ell) = f(k)f(\ell).$$

[8.4.0.7] Proposition (*Isomorphism of Infinite Cyclic Groups*). Suppose G is an infinite cyclic group. Then

$$G \cong (\mathbb{Z}, +).$$

$\therefore$

Proof. Given that G is an infinite cyclic group under multiplication, there exists $a \in G$ such that

$$G = \{a^n : n \in \mathbb{Z}\}.$$

Define

$$f : \mathbb{Z} \to G$$

by

$$f(n) = a^n.$$

Then

$$f(n+m) = a^{n+m} = a^n a^m = f(n) f(m),$$

so f is a homomorphism. If $f(m) = f(n)$, then

$$a^m = a^n,$$

so

$$a^{m-n} = 1.$$

Since G is infinite cyclic, a has infinite order. Thus

$$m - n = 0,$$

so

$$m = n.$$

Hence f is injective. It is surjective because G is generated by a. Therefore f is an isomorphism. □

[8.4.0.8] Proposition (*Isomorphism of Finite Cyclic Groups*). Suppose G is a finite cyclic group under multiplication and $\text{ord}(G) = n$. Then

$$G \cong (\mathbb{Z}_n, +).$$

$\therefore$

Proof. Given $\text{ord}(G) = n$ and G is generated by c, define

$$f : (\mathbb{Z}_n, +) \to G$$

by

$$f([a]) = c^a.$$

This is well-defined because if

$$a \equiv b \mod n,$$

then

$$n \mid (a - b),$$

so

$$c^{a-b} = 1,$$

hence

$$c^a = c^b.$$

Now

$$\begin{aligned} f([a]+[b]) &= f([a+b]) \\ &= c^{a+b} \\ &= c^a c^b \\ &= f([a])f([b]). \end{aligned}$$

Thus f is a homomorphism. If $f([a]) = f([b])$, then

$$c^a = c^b,$$

so

$$c^{a-b} = 1.$$

Since $\operatorname{ord}(c) = n$, this implies

$$n \mid (a-b),$$

hence

$$[a] = [b].$$

So f is injective. It is surjective since every element of G is of the form c^a. Therefore

$$(\mathbb{Z}_n, +) \cong G.$$

□

[8.4.0.9] Example. If p is prime, then

$$(\mathbb{Z}_p^*, \cdot) \cong (\mathbb{Z}_{p-1}, +).$$

[8.4.0.10] Proposition. If p is prime, then

$$(\mathbb{Z}_p^*, \cdot) \cong (\mathbb{Z}_{p-1}, +).$$

∴

Proof. Since $\mathbb{Z}_p^*$ is cyclic of order $p-1$, the previous proposition applies. Hence

$$\mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}.$$

□

[8.4.0.11] Definition (*Automorphism*). An isomorphism

$$f : G \to G$$

is called an automorphism.

[8.4.0.12] THEOREM (*Properties of Homomorphisms*). Let $f : G \to H$ be a group homomorphism. Then:

1. $f(1_G) = 1_H$.
2. If $a \in G$, then $f(a^{-1}) = f(a)^{-1}$.
3. $$\mathrm{Im}(f) := \{h \in H : \exists g \in G,\ f(g) = h\}$$ is a subgroup of H.
4. If f is injective, then $$\overline{f} : G \to \mathrm{Im}(f)$$ defined by $$\overline{f}(g) = f(g)$$ is an isomorphism.

Proof. **1.** Since f is a homomorphism,

$$f(1_G) = f(1_G 1_G) = f(1_G) f(1_G).$$

Multiply on the left by $f(1_G)^{-1}$ in H to get

$$1_H = f(1_G).$$

2. Since

$$aa^{-1} = 1_G,$$

we have

$$1_H = f(1_G) = f(aa^{-1}) = f(a) f(a^{-1}).$$

Thus

$$f(a^{-1}) = f(a)^{-1}.$$

3. Let $h_1, h_2 \in \mathrm{Im}(f)$. Then there exist $g_1, g_2 \in G$ such that

$$f(g_1) = h_1 \quad \text{and} \quad f(g_2) = h_2.$$

Then

$$h_1 h_2 = f(g_1) f(g_2) = f(g_1 g_2) \in \mathrm{Im}(f).$$

Also, if $h \in \mathrm{Im}(f)$, say $h = f(g)$, then by part (2),

$$h^{-1} = f(g)^{-1} = f(g^{-1}) \in \mathrm{Im}(f).$$

So $\mathrm{Im}(f) \leq H$.

4. If f is injective, then $\overline{f} : G \to \mathrm{Im}(f)$ is surjective by definition of image. It is injective because if

$$\overline{f}(g_1) = \overline{f}(g_2),$$

then

$$f(g_1) = f(g_2),$$

and injectivity of f gives

$$g_1 = g_2.$$

Since $\overline{f}$ is clearly a homomorphism, it is an isomorphism. □

[8.4.0.13] THEOREM (*Cayley's Theorem*). Every group G is isomorphic to a subgroup of a symmetric group, in fact to a subgroup of the group of permutations of G as a set.

∴

Proof. Let G be a group. For each $g \in G$, define

$$f_g : G \to G$$

by

$$f_g(x) = gx.$$

Each f_g is a permutation of G, since its inverse is $f_{g^{-1}}$. Define

$$f : G \to \mathrm{sym}(G)$$

by

$$f(g) = f_g.$$

Then f is a homomorphism because

$$f_{gh}(x) = (gh)x = g(hx) = f_g(f_h(x)).$$

So

$$f(gh) = f(g) \circ f(h).$$

We claim that f is injective. Suppose

$$f_g = f_h.$$

Then for all $x \in G$,

$$gx = hx.$$

In particular, taking $x = 1$ gives

$$g = h.$$

Thus f is injective. By the earlier theorem,

$$G \cong \mathrm{Im}(f),$$

and $\mathrm{Im}(f) \leq \mathrm{sym}(G)$. □

If G is finite and $\mathrm{ord}(G) = n$, then

$$\mathrm{sym}(G) \cong S_n.$$

So G is isomorphic to a subgroup of S_n. Note that

$$\mathrm{ord}(S_n) = n!.$$

This is called the Cayley representation. We learned the two-line notation of permutations. Now let us learn cycle notation. If

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 1 & 3 & 6 & 4 \end{pmatrix},$$

then its cycle notation is

$$(1\ 2\ 5\ 6\ 4\ 3).$$

If

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 5 & 2 \end{pmatrix},$$

then its cycle notation is

$$(1\ 3)(2\ 4\ 6),$$

and we usually omit fixed points such as (5).

[8.4.0.14] Example. If

$$\sigma = (132)(465), \qquad \tau = (23)(56),$$

then

$$\sigma\tau = (13)(46).$$

[8.4.0.15] Example. If

$$\sigma = (1345) \in S_5,$$

then

$$\sigma^2 = (14)(35).$$

[8.4.0.16] Definition (*Conjugate*). Let $g, x \in G$. Then

$$gxg^{-1}$$

is called the conjugate of x by g.

[8.4.0.17] Example. In S_3, let

$$\sigma = (123), \qquad \tau = (12).$$

Then

$$\tau\sigma\tau^{-1} = \tau\sigma\tau = (132).$$

[8.4.0.18] Example. If

$$\sigma = (13546), \qquad \tau = (245),$$

then

$$\tau^{-1} = (254),$$

and

$$\tau\sigma\tau^{-1} = (13256).$$

Conjugation preserves cycle structure. In fact,

$$\tau(a_1\ a_2\ \dots\ a_k)\tau^{-1} = (\tau(a_1)\ \tau(a_2)\ \dots\ \tau(a_k)).$$

[8.4.0.19] Definition (*Faithful*). If

$$g \mapsto f_g$$

is a homomorphism and is injective, we call the representation faithful.

[8.4.0.20] Definition (*Group of Automorphisms of G*).

$$\mathrm{Aut}(G) := \{\varphi : G \to G : \varphi \text{ is an automorphism of } G\}$$

under composition.

[8.4.0.21] Example. Define

$$\varphi : G \to \mathrm{Aut}(G)$$

by

$$g \mapsto \varphi_g, \qquad \varphi_g(x) = gxg^{-1}$$

for $x \in G$.

[8.4.0.22] Proposition. For each $g \in G$, the map

$$\varphi_g(x) = gxg^{-1}$$

is an automorphism of G, and the map

$$\varphi : G \to \mathrm{Aut}(G), \qquad g \mapsto \varphi_g$$

is a homomorphism.

$$\therefore$$

Proof. We claim $\varphi_g \in \mathrm{Aut}(G)$. For $x, y \in G$,

$$\begin{aligned}\varphi_g(xy) &= gxyg^{-1}\\ &= (gxg^{-1})(gyg^{-1})\\ &= \varphi_g(x)\varphi_g(y).\end{aligned}$$

So φ_g is a homomorphism. It is bijective because its inverse is

$$\varphi_{g^{-1}}.$$

Indeed,

$$(\varphi_g \circ \varphi_{g^{-1}})(x) = \varphi_g(g^{-1}xg) = g(g^{-1}xg)g^{-1} = x,$$

and similarly

$$\varphi_{g^{-1}} \circ \varphi_g = \mathrm{id}_G.$$

Now let $g, h \in G$. For $x \in G$,

$$\varphi_{gh}(x) = ghx(gh)^{-1}$$

$$= g(hxh^{-1})g^{-1}$$
$$= \varphi_g(\varphi_h(x)).$$

So

$$\varphi_{gh} = \varphi_g \circ \varphi_h.$$

Hence $g \mapsto \varphi_g$ is a homomorphism. □

Suppose G is abelian. Then for any $x, g \in G$,

$$\varphi_g(x) = gxg^{-1} = x.$$

So φ_g is the identity map for all $g \in G$.

[8.4.0.23] Example. Let

$$\mathrm{Inn}(G) := \{\varphi_g : g \in G\},$$

where

$$\varphi_g(x) = gxg^{-1}.$$

This is called the group of inner automorphisms of G. Prove

$$\mathrm{Inn}(G) \leq \mathrm{Aut}(G).$$

[8.4.0.24] Proposition.

$$\mathrm{Inn}(G) \leq \mathrm{Aut}(G).$$

$\therefore$

Proof. We have already shown that each $\varphi_g \in \mathrm{Aut}(G)$, so

$$\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G).$$

Since

$$g \mapsto \varphi_g$$

is a homomorphism, we have

$$\mathrm{Inn}(G) = \mathrm{Im}(\varphi),$$

which is a subgroup of $\mathrm{Aut}(G)$. □

[8.4.0.25] Example. Compute

$$\mathrm{Inn}(S_3).$$

[8.4.0.26] Example. We have

$$S_3 = \{e, (12), (13), (23), (123), (132)\}.$$

Let

$$g = (12).$$

Then

$$\varphi_g(e) = e, \qquad \varphi_g((12)) = (12),$$
$$\varphi_g((13)) = (12)(13)(12) = (23), \qquad \varphi_g((23)) = (12)(23)(12) = (13),$$
$$\varphi_g((123)) = (12)(123)(12) = (132), \qquad \varphi_g((132)) = (123).$$

So conjugation permutes the nonidentity elements of S_3 in the expected way.

In fact in this case, we can check that

$$\mathrm{Inn}(S_3) \cong \mathrm{Aut}(S_3).$$

8.5 Symmetric and Alternating Groups

[8.5.0.1] THEOREM. Every element in S_n can be written as a product of disjoint cycles.

$\therefore$

Proof. □

$$(123)(4567)$$

is disjoint.

$$(123)(426)$$

is not disjoint.

[8.5.0.2] THEOREM. Every $\omega \in S_n$ can be written as a product of transpositions.

$\therefore$

Proof. For example,

$$\begin{aligned}\sigma &= (12\dots n)\\ &= (1n)(1(n-1))\dots(13)(12).\end{aligned}$$

□

[8.5.0.3] THEOREM. Suppose $\sigma \in S_n$ with

$$\begin{aligned}\sigma &= \tau_1 \dots \tau_k, && \tau_i \text{ transpositions},\\ &= \lambda_1 \dots \lambda_r, && \lambda_i \text{ transpositions}.\end{aligned}$$

Then

$$k \equiv r \mod 2.$$

$\therefore$

Proof. Suppose $\tau = (ab)$ is a transposition. Then

$$\tau^{-1} = \tau.$$

Suppose

$$\sigma = \tau_1 \dots \tau_k$$

is a product of transpositions. Then

$$\sigma^{-1} = \tau_k \dots \tau_1.$$

First reduce to the case $\sigma = e$. Suppose

$$\sigma = \tau_1 \dots \tau_k = \lambda_1 \dots \lambda_r.$$

Then

$$1 = \sigma\sigma^{-1} = \tau_1 \dots \tau_k \lambda_r \dots \lambda_1.$$

So the identity is written as a product of $k+r$ transpositions. Thus it is enough to prove that whenever

$$e = \tau_1 \dots \tau_m,$$

the integer m is even. Assume for contradiction that

$$e = \tau_1 \dots \tau_m$$

with m odd. Choose such an expression with the fewest number of transpositions possible. Some $a \in \{1, \dots, n\}$ must appear in one of the transpositions. Among all such expressions, choose one where the leftmost occurrence of a is as far to the right as possible. Now examine the transpositions immediately around that occurrence. Using the relations among transpositions, we can commute disjoint transpositions and simplify adjacent ones. If two equal transpositions appear, they cancel. If a transposition involving a is followed by another transposition sharing exactly one element, then their product can be rewritten in a way that moves the occurrence of a farther to the right or reduces the total number of transpositions. Either way, this contradicts the minimal choice of the expression. Hence the identity cannot be written as a product of an odd number of transpositions. Therefore $k+r$ is even, so

$$k \equiv r \mod 2.$$

□

[8.5.0.4] Definition (*Sign*). The sign of σ is 1 if σ can be written as a product of an even number of transpositions, and -1 otherwise. The sign of σ is denoted by $\operatorname{sgn}(\sigma)$ or $\varepsilon(\sigma)$. The previous theorem says $\operatorname{sgn}(\sigma)$ is well-defined.

[8.5.0.5] Definition (*Even Symmetric Group*).

$$A_n := \{\sigma \in S_n : \operatorname{sgn}(\sigma) = 1\}.$$

[8.5.0.6] THEOREM. A_n is a subgroup of S_n.

$\therefore$

Proof. First, $e \in A_n$ since

$$\operatorname{sgn}(e) = 1.$$

Now let $\sigma, \tau \in A_n$. Then both σ and τ can be written as products of an even number of transpositions. Therefore $\sigma\tau$ can also be written as a product of an even number of transpositions. Hence

$$\operatorname{sgn}(\sigma\tau) = 1,$$

so $\sigma\tau \in A_n$. Also, if $\sigma \in A_n$, then σ is a product of an even number of transpositions. Since

$$\sigma^{-1}$$

is obtained by reversing that product, σ^{-1} is also a product of an even number of transpositions. Thus

$$\operatorname{sgn}(\sigma^{-1}) = 1,$$

so $\sigma^{-1} \in A_n$. Therefore $A_n \leq S_n$. □

Chapter 9

Normal Subgroups and Quotient Groups

9.1 Congruences and Lagrange's

[9.1.0.1] Definition (*Left Congruence*). Let $H \leq G$. Define a relation on G by

$$a \sim b, \qquad a \overset{\ell}{\sim} b \mod H$$

if

$$a^{-1}b \in H.$$

Equivalently,

$$b^{-1}a \in H.$$

This is called left congruence modulo H.

[9.1.0.2] Theorem. Left congruence is an equivalence relation.

$\therefore$

Proof. **1)** It is reflexive. If $a \in G$, then

$$a^{-1}a = e \in H.$$

2) Let $a, b \in G$. Then

$$a \sim b \iff a^{-1}b \in H.$$

Since H is closed under inverses,

$$a^{-1}b \in H \iff (a^{-1}b)^{-1} \in H \iff b^{-1}a \in H.$$

Thus

$$a \sim b \iff b \sim a.$$

Hence $\sim$ is symmetric.

3) Suppose $a, b, c \in G$ and $a \sim b$, $b \sim c$. Then

$$a^{-1}b \in H \quad \text{and} \quad b^{-1}c \in H.$$

So

$$(a^{-1}b)(b^{-1}c) = a^{-1}c \in H.$$

Thus

$$a \sim c.$$

Hence $\sim$ is transitive. □

What are the left equivalence classes?

[9.1.0.3] Definition (*Left Congruence Classes*). The left congruence class of a is

$$\{b \in G : b \equiv a \mod H\} = \{b \in G : \exists h \in H,\ b = ah\} = aH = \{ah : h \in H\}.$$

We call aH the left coset containing a. These partition G. That is, G is the union of its left cosets, and any two left cosets are either identical or disjoint.

Suppose

$$G = S_3 \quad \text{and} \quad H = \langle (12) \rangle = \{e, (12)\}.$$

Then

$$(13)H = \{(13), (132)\},$$
$$(23)H = \{(23), (123)\}.$$

Thus

$$S_3 = \{e, (12)\} \cup \{(13), (132)\} \cup \{(23), (123)\}.$$

[9.1.0.4] Proposition. All left cosets of H have $\#H$ elements.

∴

Proof. Let $a \in G$. Then

$$aH = \{ah : h \in H\}$$

is a left coset of H in G. Define a map

$$\varphi : H \to aH$$

by

$$\varphi(h) = ah.$$

This map is injective, since

$$ah_1 = ah_2 \implies h_1 = h_2$$

by cancellation in G. It is also surjective by definition of aH. So φ is a bijection. Hence

$$\#H = \#aH.$$

Note that aH need not be a group. This is only a set bijection. □

[9.1.0.5] Definition (*Index of H in G*). The number of distinct left cosets of H in G is called the index of H in G, denoted by

$$[G : H].$$

If G is finite, then

$$[G : H] = \frac{\text{ord}(G)}{\text{ord}(H)}.$$

[9.1.0.6] Theorem (*Lagrange's Theorem*). Suppose G is a finite group. If $H \leq G$, then

$$\text{ord}(H) \mid \text{ord}(G).$$

$\therefore$

Proof. Suppose

$$G = a_1 H \cup \cdots \cup a_k H,$$

where the $a_i H$ are the distinct left cosets of H in G. Then

$$k = [G : H].$$

Each coset has $\text{ord}(H)$ elements. So

$$\text{ord}(G) = k\text{ord}(H).$$

Therefore

$$\text{ord}(H) \mid \text{ord}(G).$$

□

[9.1.0.7] Corollary (*Corollary of Lagrange's Theorem*). Suppose G is a finite group of prime order. If $H \leq G$, then

$$H = \{e\} \quad \text{or} \quad H = G.$$

$\therefore$

Proof. Since $\text{ord}(H) \mid \text{ord}(G)$ and $\text{ord}(G) = p$ is prime, we must have

$$\text{ord}(H) = 1 \quad \text{or} \quad \text{ord}(H) = p.$$

Hence

$$H = \{e\} \quad \text{or} \quad H = G.$$

□

[9.1.0.8] Corollary (*Corollary of the Previous Corollary*). Suppose G is a finite group of prime order. Then G is cyclic. In fact,

$$G \cong (\mathbb{Z}_p, +).$$

$\therefore$

Proof. Let $1 \neq a \in G$. Let

$$H = \langle a \rangle.$$

Then H is a subgroup of G and is not trivial. By the previous corollary, we must have

$$H = G.$$

So G is cyclic. Since $\text{ord}(G) = p$, we get

$$G \cong (\mathbb{Z}_p, +).$$

□

[9.1.0.9] Corollary (*Corollary of Fermat's Little Theorem*). Let p be prime, $a \in \mathbb{Z}$, and $p \nmid a$. Then

$$a^{p-1} \equiv 1 \mod p.$$

$\therefore$

Proof. Let

$$G = \mathbb{Z}_p^*.$$

Then $[a] \in \mathbb{Z}_p^*$. By Lagrange's Theorem,

$$\text{ord}(\langle [a] \rangle) \mid (p-1).$$

Hence

$$[a]^{p-1} = [1]$$

in $\mathbb{Z}_p^*$. Therefore

$$a^{p-1} \equiv 1 \mod p.$$

□

[9.1.0.10] Corollary (*Corollary 2 of Fermat's Little Theorem*). For all $a \in \mathbb{Z}$,

$$a^p \equiv a \mod p.$$

Thus

$$\frac{a^p - a}{p} \in \mathbb{Z}.$$

$\therefore$

Proof. If $p \mid a$, then

$$a \equiv 0 \mod p,$$

so

$$a^p \equiv 0 \equiv a \mod p.$$

If $p \nmid a$, then by Fermat's Little Theorem,

$$a^{p-1} \equiv 1 \mod p.$$

Multiplying by a gives

$$a^p \equiv a \mod p.$$

Thus in all cases,

$$p \mid (a^p - a),$$

so

$$\frac{a^p - a}{p} \in \mathbb{Z}.$$

□

[9.1.0.11] Example. Suppose $\operatorname{ord}(G) = 4$. Let $1 \neq a \in G$. Since

$$\operatorname{ord}(\langle a \rangle) \mid 4,$$

we have

$$\operatorname{ord}(\langle a \rangle) = 2 \quad \text{or} \quad \operatorname{ord}(\langle a \rangle) = 4.$$

If $\operatorname{ord}(a) = 4$, then G is cyclic and

$$G \cong \mathbb{Z}_4.$$

Suppose instead that every nonidentity element has order 2. Let $1 \neq a, b \in G$ with $a \neq b$. Then

$$G = \{1, a, b, ab\}.$$

In this case,

$$G \cong C_2 \times C_2,$$

the Klein-4 group.

9.2 Normal Subgroups

We have previously defined left congruence as follows. Let $H \leq G$ and $a, b \in G$. Then

$$a \overset{\ell}{\equiv} b \mod H$$

if

$$a^{-1} b \in H.$$

We also defined left cosets as

$$aH := \{ah : h \in H\}.$$

[9.2.0.1] Definition (*Right Congruence*). Let $H \leq G$. Define

$$a \overset{r}{\equiv} b \mod H$$

if

$$ba^{-1} \in H.$$

Equivalently,

$$ab^{-1} \in H.$$

This defines an equivalence relation. The equivalence classes are called right cosets and are given by

$$Ha := \{ha : h \in H\}.$$

Note that

$$a \in aH \cap Ha,$$

but this may be the only common element. In general,

$$aH \neq Ha.$$

[9.2.0.2] Example. Let

$$G = S_3, \quad H = \{e, (12)\} = \langle (12) \rangle.$$

Left cosets:

$$H = \{e, (12)\}, \quad (13)H = \{(13), (132)\}, \quad (23)H = \{(23), (123)\}.$$

Right cosets:

$$H = \{e, (12)\}, \quad H(13) = \{(13), (123)\}, \quad H(23) = \{(23), (132)\}.$$

[9.2.0.3] Example. Let

$$N = \{e, (123), (132)\} = \langle (123) \rangle.$$

Left cosets:

$$N, \quad (12)N = \{(12), (23), (13)\} = (23)N = (13)N.$$

Right cosets:

$$N, \quad N(12).$$

Thus

$$[G : N] = 2.$$

Recall that the number of left cosets always equals the number of right cosets:

$$[G : H] = \frac{\text{ord}(G)}{\text{ord}(H)}.$$

[9.2.0.4] Definition (*Normal Subgroup*). Let $N \leq G$. We say N is normal in G if the left cosets equal the right cosets. This is denoted by

$$N \trianglelefteq G.$$

That is,

$$aN = Na \quad \text{for all } a \in G.$$

[9.2.0.5] Theorem. Let $N \leq G$. The following are equivalent:

1. The set of left cosets equals the set of right cosets.

2. For all $a \in G$, $aN = Na$.
3. For all $a \in G$, $aNa^{-1} = N$.
4. For all $a \in G$, $a^{-1}Na = N$.
5. For all $a \in G$ and $x \in N$, $axa^{-1} \in N$.
6. For all $a \in G$ and $x \in N$, $a^{-1}xa \in N$.
7. Multiplication of left cosets is well-defined, i.e.
$$(aN)(bN) = abN.$$
8. Multiplication of right cosets is well-defined.

$\therefore$

Proof. □

Proof. We sketch key implications.

(2) $\Longrightarrow$ (1) is immediate.

(1) $\Longrightarrow$ (2): If left and right cosets coincide, then for any $a \in G$, the left coset aN must equal the right coset containing a, so $aN = Na$.

(2) $\Longrightarrow$ (5): Let $x \in N$. Then $ax \in aN = Na$, so $ax = ya$ for some $y \in N$. Thus
$$axa^{-1} = y \in N.$$

(5) $\Longrightarrow$ (4): For all $x \in N$, we have $axa^{-1} \in N$, so $aNa^{-1} \subseteq N$. Applying the same argument with a^{-1} gives equality.

(2) $\Longrightarrow$ (7): Suppose $aN = cN$ and $bN = dN$. Then $c^{-1}a \in N$ and $d^{-1}b \in N$. Using normality,
$$d^{-1}c^{-1}ab \in N,$$
so
$$abN = cdN.$$
Thus coset multiplication is well-defined. ■

[9.2.0.6] THEOREM. If $N \trianglelefteq G$, then multiplication of cosets is well-defined. That is, if $aN = cN$ and $bN = dN$, then
$$abN = cdN.$$

$\therefore$

Proof. □

Proof. If $aN = cN$, then $c^{-1}a \in N$. If $bN = dN$, then $d^{-1}b \in N$. Since N is normal,

$$d^{-1}(c^{-1}a)d \in N.$$

Multiplying,

$$(d^{-1}(c^{-1}a)d)(d^{-1}b) = d^{-1}c^{-1}ab \in N.$$

Thus

$$(cd)^{-1}ab \in N,$$

so $abN = cdN$. ■

[9.2.0.7] Proposition. $N \trianglelefteq G$ if and only if for all $a \in G$ and $x \in N$,

$$axa^{-1} \in N.$$

∴

Proof. □

Proof. ($\Longrightarrow$) If N is normal, then $aN = Na$. So for $x \in N$, $ax \in Na$, hence $ax = ya$ for some $y \in N$. Thus

$$axa^{-1} = y \in N.$$

($\Longleftarrow$) If $axa^{-1} \in N$ for all $a \in G$ and $x \in N$, then $aN \subseteq Na$. A similar argument gives $Na \subseteq aN$, so $aN = Na$. ■

[9.2.0.8] Definition (*Characteristic Subgroup*). A subgroup $N \leq G$ is characteristic in G if for every automorphism $\varphi \in \mathrm{Aut}(G)$,

$$\varphi(N) = N.$$

This is denoted by

$$N\mathit{charG}.$$

[9.2.0.9] Lemma. If $N\mathit{charG}$, then $N \trianglelefteq G$.

∴

Proof. □

[9.2.0.10] Lemma. The center of G is characteristic in G.

∴

Proof. □

[9.2.0.11] Definition (*Quotient Group*). Let $N \trianglelefteq G$. The quotient group is

$$G/N := \{gN : g \in G\}.$$

The operation is defined by

$$(gN)(hN) = ghN.$$

9.3 Homomorphisms and Isomorphisms

[9.3.0.1] Definition (*Center*).

$$Z(G) := \{x \in G : xa = ax \ \forall a \in G\} = \{x \in G : xax^{-1} = a \ \forall a \in G\} = \bigcap_{a \in G} C_G(a).$$

Note that the centralizer is only for one element a:

$$C_G(a) := \{x \in G : xa = ax\}.$$

Also,

$$Z(G) \trianglelefteq G.$$

[9.3.0.2] Theorem. Suppose $G/Z(G)$ is cyclic. Then G is abelian. Hence $Z(G) = G$.

$\therefore$

Proof. Denote $Z(G) = Z$. Let cZ be a generator for G/Z. Then every coset in G/Z has the form

$$aZ = c^i Z, \qquad bZ = c^j Z$$

for some $i, j \in \mathbb{Z}$. Let $a \in c^i Z$ and $b \in c^j Z$. Then there exist $d, e \in Z$ such that

$$a = c^i d, \qquad b = c^j e.$$

Thus

$$\begin{aligned} ab &= c^i d c^j e \\ &= c^i c^j de \\ &= c^i c^j ed \\ &= c^{i+j} ed \\ &= c^{j+i} de \\ &= c^j c^i de \\ &= c^j ec^i d \\ &= ba. \end{aligned}$$

So $ab = ba$ for all $a, b \in G$. Therefore G is abelian. Hence $Z(G) = G$. □

[9.3.0.3] Definition (*Kernel of Group Functions*). Suppose $\varphi : G \to H$ is a group homomor-

phism. Define the kernel of φ by

$$\ker\varphi := \{g \in G : \varphi(g) = 1_H\}.$$

[9.3.0.4] Proposition.

$$\ker\varphi \trianglelefteq G.$$

Also, φ is injective if and only if

$$\ker\varphi = \{1_G\}.$$

$\therefore$

Proof. First, $1_G \in \ker\varphi$ since

$$\varphi(1_G) = 1_H.$$

If $a, b \in \ker\varphi$, then

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = 1_H 1_H^{-1} = 1_H.$$

So $ab^{-1} \in \ker\varphi$. Hence $\ker\varphi \leq G$. Now let $g \in G$ and $x \in \ker\varphi$. Then

$$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)1_H\varphi(g)^{-1} = 1_H.$$

Thus

$$gxg^{-1} \in \ker\varphi.$$

So

$$\ker\varphi \trianglelefteq G.$$

Now suppose φ is injective. If $r \in \ker\varphi$, then

$$\varphi(r) = 1_H = \varphi(1_G).$$

Since φ is injective, $r = 1_G$. Thus

$$\ker\varphi = \{1_G\}.$$

Conversely, suppose

$$\ker\varphi = \{1_G\}.$$

If $\varphi(r) = \varphi(s)$, then

$$\varphi(rs^{-1}) = \varphi(r)\varphi(s)^{-1} = 1_H.$$

So

$$rs^{-1} \in \ker\varphi.$$

Hence

$$rs^{-1} = 1_G,$$

so $r = s$. Therefore φ is injective. □

[9.3.0.5] Theorem (*First Isomorphism Theorem*). Suppose $\varphi : G \to H$ is a group homomorphism. Let $K = \ker\varphi$. Then

$$G/K \cong \mathrm{Im}(\varphi).$$

Define

$$\overline{\varphi} : G/K \to \mathrm{Im}(\varphi)$$

by

$$\overline{\varphi}(gK) = \varphi(g).$$

Then $\overline{\varphi}$ is a well-defined injective homomorphism whose image is $\mathrm{Im}(\varphi)$.

$\therefore$

Proof. To show $\overline{\varphi}$ is well-defined, suppose

$$gK = hK.$$

Then

$$h^{-1}g \in K = \ker\varphi.$$

So

$$\varphi(h^{-1}g) = 1_H.$$

Hence

$$\varphi(h)^{-1}\varphi(g) = 1_H,$$

which implies

$$\varphi(g) = \varphi(h).$$

Thus $\overline{\varphi}(gK) = \overline{\varphi}(hK)$. Now for $gK, hK \in G/K$,

$$\overline{\varphi}((gK)(hK)) = \overline{\varphi}(ghK) = \varphi(gh) = \varphi(g)\varphi(h) = \overline{\varphi}(gK)\overline{\varphi}(hK).$$

So $\overline{\varphi}$ is a homomorphism. It is injective because if

$$\overline{\varphi}(gK) = 1_H,$$

then

$$\varphi(g) = 1_H,$$

so $g \in K$. Hence $gK = K$. Thus

$$\ker(\overline{\varphi}) = \{K\},$$

so $\overline{\varphi}$ is injective. Its image is exactly $\mathrm{Im}(\varphi)$ by definition. Therefore

$$G/K \cong \mathrm{Im}(\varphi).$$

□

Let

$$f : G/K \to \mathrm{Im}(\varphi)$$

be given by

$$f(gK) = \varphi(g).$$

This is the isomorphism from the theorem.

[9.3.0.6] Theorem. The map

$$g \mapsto \varphi_g$$

is a homomorphism from G to (G), where

$$\varphi_g(x) = gxg^{-1}.$$

$\therefore$

Proof. Let $a, b \in G$. We need to check that

$$\varphi_{ab} = \varphi_a \circ \varphi_b.$$

Let $x \in G$. Then

$$\begin{aligned} \varphi_{ab}(x) &= abx(ab)^{-1} \\ &= abxb^{-1}a^{-1} \\ &= a\varphi_b(x)a^{-1} \\ &= \varphi_a(\varphi_b(x)). \end{aligned}$$

So

$$\varphi_{ab} = \varphi_a \circ \varphi_b.$$

Hence

$$g \mapsto \varphi_g$$

is a homomorphism. Now compute its kernel. We have

$$\ker\varphi = \{y \in G : \varphi_y(x) = x \ \forall x \in G\}.$$

This means

$$yxy^{-1} = x \quad \forall x \in G.$$

Equivalently,

$$yx = xy \quad \forall x \in G.$$

So

$$\ker\varphi = Z(G).$$

□

[9.3.0.7] Corollary.

$$G/Z(G) \cong (G).$$

$\therefore$

Proof. This follows from the first isomorphism theorem applied to the homomorphism

$$G \to (G), \qquad g \mapsto \varphi_g.$$

Its kernel is $Z(G)$, and its image is (G). Hence

$$G/Z(G) \cong (G).$$

□

If G is abelian, then

$$Z(G) = G$$

and

$$(G) = \{\mathrm{id}\}.$$

If $G = S_n$ with $n \geq 3$, then

$$Z(G) = \{1\},$$

so

$$G \cong (G) \leq (G).$$

Thus

$$(G) \trianglelefteq (G).$$

[9.3.0.8] THEOREM. Suppose

$$K \trianglelefteq N \trianglelefteq G$$

with also

$$K \trianglelefteq G.$$

Then

$$N/K \trianglelefteq G/K$$

and

$$(G/K)/(N/K) \cong G/N.$$

Proof. Define

$$\varphi : G/K \to G/N$$

by

$$\varphi(gK) = gN.$$

First check that φ is well-defined. Suppose

$$aK = bK.$$

Then

$$b^{-1}a \in K.$$

Since

$$K \leq N,$$

we have

$$b^{-1}a \in N.$$

Thus

$$aN = bN.$$

Now compute the kernel. Suppose

$$gK \in \ker\varphi.$$

Then

$$\varphi(gK) = N.$$

So

$$gN = N,$$

which means

$$g \in N.$$

Hence

$$gK \in N/K.$$

Thus

$$\ker\varphi = N/K.$$

Also, φ is surjective, since for any $gN \in G/N$,

$$\varphi(gK) = gN.$$

Therefore, by the first isomorphism theorem,

$$(G/K)/(N/K) \cong G/N.$$

Since $N/K = \ker\varphi$, it is normal in G/K. Thus

$$N/K \trianglelefteq G/K.$$

□

Normality is not transitive. It is possible that

$$K \trianglelefteq N \quad \text{and} \quad N \trianglelefteq G$$

but

$$K \not\trianglelefteq G.$$

For example, if

$$G = \mathbb{Z}, \qquad N = 6\mathbb{Z}, \qquad K = 12\mathbb{Z},$$

then

$$K \trianglelefteq N \trianglelefteq G \quad \text{and} \quad K \trianglelefteq G.$$

Also,

$$G/N = \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6,$$
$$N/K = 6\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}_2,$$
$$G/K = \mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}_{12},$$

and

$$(G/K)/(N/K) \cong \mathbb{Z}_6 \cong G/N.$$

[9.3.0.9] THEOREM (*4th Isomorphism Theorem*). Suppose

$$N \trianglelefteq G.$$

Then there is a bijection between subgroups of G/N and subgroups of G containing N.

∴

Proof. Suppose $H \leq G$ with $N \leq H$. Define

$$T = \{hN : h \in H\}.$$

We check that $T \leq G/N$. Since $1 \in H$, we have

$$N = 1N \in T.$$

If $h_1, h_2 \in H$, then

$$(h_1N)(h_2N) = (h_1h_2)N \in T.$$

If $h \in H$, then

$$(hN)^{-1} = h^{-1}N \in T.$$

So $T \leq G/N$. Conversely, suppose $T \leq G/N$. Define

$$H = \{h \in G : hN \in T\}.$$

We check that $H \leq G$. Since $N \in T$, we have $1 \in H$. If $h_1, h_2 \in H$, then

$$h_1N, h_2N \in T.$$

Since T is a group,

$$(h_1N)(h_2N) = (h_1h_2)N \in T.$$

So $h_1h_2 \in H$. If $h \in H$, then

$$hN \in T,$$

so

$$(hN)^{-1} = h^{-1}N \in T.$$

Thus $h^{-1} \in H$. Hence $H \leq G$. These maps are inverse to each other, so the correspondence is a bijection. □

These maps are also inverses of one another. If we start with $H \leq G$ containing N, then

$$T = \{hN : h \in H\}.$$

If we start with $T \leq G/N$, then

$$H = \{h \in G : hN \in T\}.$$

[9.3.0.10] Proposition. Under these maps,

$$H \trianglelefteq G \iff T \trianglelefteq G/N.$$

∴

Proof. ($\Longrightarrow$). Let $xN \in T$ and $gN \in G/N$. Then

$$(gN)(xN)(g^{-1}N) = gxg^{-1}N.$$

Since $H \trianglelefteq G$ and $x \in H$, we have

$$gxg^{-1} \in H.$$

Thus

$$gxg^{-1}N \in T.$$

So

$$T \trianglelefteq G/N.$$

($\Longleftarrow$). Suppose $T \trianglelefteq G/N$. Let $x \in H$ and $g \in G$. Since $xN \in T$, we have

$$(gN)(xN)(g^{-1}N) \in T.$$

That is,

$$gxg^{-1}N \in T.$$

Hence

$$gxg^{-1} \in H.$$

So

$$H \trianglelefteq G.$$

□

[9.3.0.11] Definition (*Simple Group*). Suppose G is a group and

$$\{1\} \neq G.$$

We say G is simple if and only if

$$N \trianglelefteq G$$

implies

$$N = G \quad \text{or} \quad N = \{1\}.$$

[9.3.0.12] Theorem. If G is abelian and simple, then

$$G \cong C_p$$

for some prime p.

∴

Proof. Since G is abelian, every subgroup is normal. Because G is simple, it has no proper nontrivial subgroups. Take

$$1 \neq a \in G.$$

Then

$$\langle a \rangle \leq G.$$

Since $\langle a \rangle \neq \{1\}$ and G is simple, we must have

$$\langle a \rangle = G.$$

Thus G is cyclic.

So

$$G \cong C_n$$

for some n. If n were composite, then there would exist a proper nontrivial subgroup of C_n, namely

$$\langle a^k \rangle$$

for a suitable divisor k of n. But that would contradict simplicity. Therefore n must be prime. Hence

$$G \cong C_p$$

for some prime p. □

What does it mean when a group is not simple. It means it has a proper normal subgroup. Suppose

G is not simple. Then

$$1 \neq N \triangleleft G.$$

Thus one studies the quotient G/N and can lift proper normal subgroups of G/N back to G. Now the correct thing to ask is what lift means.

[9.3.0.13] Definition (*Lift*). By the 4th Isomorphism Theorem, there is a bijection between subgroups

$$T \leq G/N$$

and subgroups

$$H \leq G$$

containing N. We lift T by assigning to it its corresponding subgroup H in G.

[9.3.0.14] Definition (*Jordan–Holder Series / Composition Series*). If G is not simple, we may find a proper normal subgroup $N \triangleleft G$. Then we may continue by finding a proper normal subgroup of G/N, and so on. Eventually we run out of proper normal subgroups. This process creates a sequence

$$\{1\} \leq G_1 \leq G_2 \leq \cdots \leq G_n \leq G$$

with

$$G_i \trianglelefteq G_{i+1}$$

and each quotient

$$G_{i+1}/G_i$$

simple. This sequence is called a Jordan–Holder series, or composition series.

[9.3.0.15] Example. Let

$$G = C_6 \cong C_3 \times C_2.$$

Then

$$N_1 = C_3 \times \{1\} \trianglelefteq G$$

and

$$N_2 = \{1\} \times C_2 \trianglelefteq G.$$

Thus

$$G/N_1 \cong C_2$$

and

$$G/N_2 \cong C_3.$$

So we have two composition series:

$$\{1\} \trianglelefteq N_1 \trianglelefteq G$$

and

$$\{1\} \trianglelefteq N_2 \trianglelefteq G.$$

Their composition factors are the same up to order:

$$N_1/\{1\} \cong C_3, \qquad G/N_1 \cong C_2,$$

and

$$N_2/\{1\} \cong C_2, \qquad G/N_2 \cong C_3.$$

9.4 Simplicity of A_n

[9.4.0.1] THEOREM. If $n \geq 5$, then A_n is simple.

$\therefore$

Proof. Outline of proof.

1. A_n is generated by 3-cycles. Indeed, every element of A_n is, by definition, a product of an even number of transpositions. Every pair of transpositions is of one of the following forms:

$$(ab)(cd), \qquad (ab)(ac), \qquad (ab)(ab).$$

In the first case,

$$(ab)(cd) = (adb)(adc).$$

In the second case,

$$(ab)(ac) = (acb).$$

In the third case,

$$(ab)(ab) = e = (abc)(acb).$$

Thus every pair of transpositions is either a 3-cycle or a product of two 3-cycles. Hence every element of A_n is a product of 3-cycles.

2. Suppose $N \trianglelefteq A_n$ and $(123) \in N$. Then N contains every 3-cycle. Indeed, since N is normal, for every $x \in A_n$,

$$x(123)x^{-1} \in N.$$

But conjugation preserves cycle structure, and

$$x(123)x^{-1} = (x(1)\ x(2)\ x(3)).$$

Since every 3-cycle in A_n is of this form, N contains all 3-cycles. Because A_n is generated by 3-cycles, this implies

$$N = A_n.$$

3. Now suppose $1 \neq N \trianglelefteq A_n$. We show that N contains a 3-cycle. Take

$$1 \neq \sigma \in N.$$

Write σ as a product of disjoint cycles. If one of the disjoint cycles has length at least 3, say

$$(123\ldots r)$$

with $r \geq 3$, let

$$\tau = (123).$$

Then the commutator

$$\tau\sigma\tau^{-1}\sigma^{-1} \in N$$

since N is normal. A direct computation shows that this produces a 3-cycle. For example, when the support is chosen appropriately, one gets an element such as

$$(1\,2\,4) \in N.$$

If instead σ is a product only of disjoint 2-cycles, then because $\sigma \in A_n$, there are an even number of them. Since $n \geq 5$, after relabeling we may assume

$$\sigma = (1\,2)(3\,4)\cdots.$$

Let

$$\tau = (1\,2\,3) \in A_n.$$

Then again the commutator

$$\tau\sigma\tau^{-1}\sigma^{-1} \in N$$

is a 3-cycle. Thus in every case, N contains a 3-cycle. By Step 2, it follows that

$$N = A_n.$$

Therefore A_n is simple for all $n \geq 5$. □

[9.4.0.2] THEOREM. For each $n \geq 5$, the alternating group A_n is simple. Also, A_3 is simple.

$\therefore$

Proof. The case $n \geq 5$ is the previous theorem. Also,

$$A_3 = \{e, (123), (132)\},$$

so

$$\mathrm{ord}(A_3) = 3.$$

Since 3 is prime, any subgroup of A_3 has order 1 or 3 by Lagrange's Theorem. Thus A_3 has no nontrivial proper normal subgroups. Hence A_3 is simple. Note that A_1 and A_2 are trivial, so they are not simple under our definition, and A_4 is not simple. □

Chapter 10

Topics in Group Theory

10.1 Direct Sums and Finite Abelian Groups

[10.1.0.1] Definition (*External Direct Product*). Let H, K be groups. Define

$$G = H \times K = \{(h,k) : h \in H,\ k \in K\}.$$

Then G is a group under componentwise operation. Also,

$$\overline{H} = \{(h,1) : h \in H\} \trianglelefteq G$$

and

$$\overline{K} = \{(1,k) : k \in K\} \trianglelefteq G.$$

In fact,

$$\overline{H} \cap \overline{K} = \{(1,1)\}.$$

[10.1.0.2] Theorem. Suppose G is a group and $H, K \leq G$. When is G isomorphic to the direct product of H and K.

$\therefore$

Proof. This happens when H and K are normal in G, when

$$H \cap K = \{1\},$$

and when

$$G = HK.$$

□

[10.1.0.3] Remark. Define

$$HK := \{hk : h \in H,\ k \in K\}.$$

If $H, K \trianglelefteq G$, then HK is a subgroup of G.

[10.1.0.4] Theorem. If $H, K \trianglelefteq G$, $G = HK$, and

$$H \cap K = \{1\},$$

then

$$G \cong H \times K.$$

This is called an internal direct product.

$\therefore$

Proof. Define

$$\varphi : H \times K \to G$$

by

$$\varphi(h,k) = hk.$$

Since $G = HK$, φ is surjective. To show φ is a homomorphism, let $(h_1,k_1),(h_2,k_2) \in H \times K$. Because H and K are normal and $H \cap K = \{1\}$, elements of H commute with elements of K. Indeed, for $h \in H$ and $k \in K$,

$$hkh^{-1}k^{-1} \in H \cap K = \{1\},$$

so $hk = kh$. Thus

$$\begin{aligned}\varphi((h_1,k_1)(h_2,k_2)) &= \varphi(h_1h_2, k_1k_2)\\ &= (h_1h_2)(k_1k_2)\\ &= h_1k_1h_2k_2\\ &= \varphi(h_1,k_1)\varphi(h_2,k_2).\end{aligned}$$

Now compute the kernel. If

$$\varphi(h,k) = 1,$$

then

$$hk = 1,$$

so

$$h = k^{-1}.$$

Hence $h \in H \cap K$ and $k \in H \cap K$. Since

$$H \cap K = \{1\},$$

we get

$$h = k = 1.$$

Thus

$$\ker\varphi = \{(1,1)\}.$$

So φ is injective. Therefore φ is an isomorphism. □

[10.1.0.5] Definition (*Disjoint Group*). If

$$H \cap K = \{1\},$$

we say the intersection is trivial.

[10.1.0.6] Example (*Example 1*). Let

$$G = \langle x \rangle, \qquad \operatorname{ord}(x) = n.$$

Proof. Suppose

$$n = ab, \qquad \gcd(a, b) = 1.$$

Let

$$H = \langle x^a \rangle, \qquad K = \langle x^b \rangle.$$

Then

$$H \cong C_b, \qquad K \cong C_a.$$

If $x^r \in H \cap K$, then $a \mid r$ and $b \mid r$. Since $\gcd(a, b) = 1$, this implies

$$ab = n \mid r.$$

Hence

$$x^r = 1.$$

So

$$H \cap K = \{1\}.$$

Now let $r \in \mathbb{Z}$. Since $\gcd(a, b) = 1$, there exist $s, t \in \mathbb{Z}$ such that

$$r = sa + tb.$$

Then

$$\begin{aligned} x^r &= x^{sa+tb} \\ &= x^{sa} x^{tb} \\ &= (x^a)^s (x^b)^t. \end{aligned}$$

So $x^r \in HK$ for all r. Hence

$$G = HK.$$

Therefore

$$G \cong H \times K.$$

■

[10.1.0.7] Definition (*Direct Sum*). When G is an additive abelian group, the direct product is called a direct sum.

[10.1.0.8] Theorem (*Fundamental Theorem*). If G is a finite abelian group, then G can be written in the following equivalent ways:

1.

$$G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}.$$

2.
$$G \cong \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_1^{k_2}} \oplus \mathbb{Z}_{p_2^{\ell_1}} \oplus \cdots.$$

3.
$$G \cong \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_k},$$

where the $p_i^{k_j}$ are the elementary divisors and the d_i are the invariant factors.

$\therefore$

Proof. □

[10.1.0.9] Remark. The implication from elementary divisors to invariant factors uses the fact that if
$$\gcd(m,n) = 1,$$
then
$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n.$$

[10.1.0.10] Example. Let
$$G = \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5.$$
The primes involved are $2,3,5$. Taking one highest available power of each prime gives
$$2^2 \cdot 3 \cdot 5 = 60 = d_3.$$
Removing those factors leaves
$$2^2 \cdot 3 \cdot 1 = 12 = d_2.$$
Removing again leaves
$$2 \cdot 1 \cdot 1 = 2 = d_1.$$
So
$$G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{60}.$$

[10.1.0.11] Remark. One way to begin proving the theorem is as follows. Suppose $x_1, \ldots, x_n$ generate G. Define a surjective homomorphism
$$\varphi : \mathbb{Z}^n \to G$$
by sending
$$e_i \mapsto x_i,$$
where
$$e_1 = (1,0,\ldots,0), \quad e_2 = (0,1,0,\ldots,0), \quad \ldots, \quad e_n = (0,0,\ldots,1).$$
Then every
$$y = y_1 e_1 + \cdots + y_n e_n \in \mathbb{Z}^n$$

maps to

$$\sum_{i=1}^{n} y_i x_i.$$

If

$$K = \ker \varphi,$$

then by the first isomorphism theorem,

$$\mathbb{Z}^n / K \cong G.$$

So the problem reduces to understanding subgroups of $\mathbb{Z}^n$.

[10.1.0.12] Definition (*Free Abelian Group*). A group G is a free abelian group if it has a basis.

[10.1.0.13] Remark. Recall from Linear Algebra. A basis for $\mathbb{Z}^n$ is

$$e_1, \ldots, e_n,$$

which generates $\mathbb{Z}^n$ and is linearly independent over $\mathbb{Z}$.

[10.1.0.14] Lemma. Every subgroup of $\mathbb{Z}^n$ has a basis.

$\therefore$

Proof. □

A direct product and direct sum are similar in spirit to bases, but now for groups.

[10.1.0.15] Theorem. A set

$$\{f_1, \ldots, f_m\}$$

is a basis for a subgroup $K \leq \mathbb{Z}^n$ if every $k \in K$ can be written as

$$k = \sum a_i f_i$$

with $a_i \in \mathbb{Z}$, and if

$$\sum a_i f_i = 0$$

implies $a_i = 0$ for all i.

$\therefore$

Proof. □

We want to show that every element k can be written as such a linear combination.

[10.1.0.16] Theorem. Every subgroup of $\mathbb{Z}^n$ is free abelian.

$\therefore$

Proof. We prove this by induction on n. Base case: $n = 1$. Every subgroup of $\mathbb{Z}$ is cyclic. If

$$K \neq \{0\}$$

is a subgroup of $\mathbb{Z}$, then

$$K = d\mathbb{Z}$$

for some $d \neq 0$. So

$$\{d\}$$

is a basis for K. Thus every subgroup of $\mathbb{Z}$ has a basis. Now consider $n = 2$. Let

$$K \leq \mathbb{Z}^2 = \mathbb{Z}e_1 + \mathbb{Z}e_2.$$

If

$$K \leq \mathbb{Z}e_1,$$

then we are done by the $n = 1$ case. Assume not. Let

$$H := \{b \in \mathbb{Z} : \exists y \in \mathbb{Z} \text{ such that } (y, b) = ye_1 + be_2 \in K\}.$$

Then H is a subgroup of $\mathbb{Z}$. Since

$$K \not\leq \mathbb{Z}e_1,$$

we have

$$H \neq \{0\}.$$

So

$$H = d\mathbb{Z}$$

for some $d \neq 0$. Thus there exists $y_1 \in \mathbb{Z}$ such that

$$(y_1, d) = y_1 e_1 + de_2 \in K.$$

Let

$$f_2 = (y_1, d).$$

Also,

$$K \cap \mathbb{Z}e_1$$

is a subgroup of $\mathbb{Z}e_1 \cong \mathbb{Z}$. If

$$K \cap \mathbb{Z}e_1 = \{(0, 0)\},$$

then one basis vector may suffice. Otherwise,

$$K \cap \mathbb{Z}e_1 = \mathbb{Z}(a, 0)$$

for some $a \neq 0$. Let

$$f_1 = (a, 0).$$

Then the claim is that either $\{f_2\}$ or $\{f_1, f_2\}$ is a basis for K. □

[10.1.0.17] Lemma. If

$$K \cap \mathbb{Z}e_1 = \{(0, 0)\},$$

then $\{f_2\}$ is a basis for K. If

$$K \cap \mathbb{Z}e_1 = \mathbb{Z}(a, 0),$$

then $\{f_1, f_2\}$ is a basis for K.

$\therefore$

Proof. Let

$$k = (z_1, z_2) \in K.$$

Since $z_2 \in H = d\mathbb{Z}$, there exists $k_2 \in \mathbb{Z}$ such that

$$z_2 = d\,k_2.$$

Then

$$\begin{aligned} k - k_2 f_2 &= (z_1, z_2) - k_2(y_1, d) \\ &= (z_1 - k_2 y_1, z_2 - k_2 d) \\ &= (z_1 - k_2 y_1, 0). \end{aligned}$$

Thus

$$k - k_2 f_2 \in K \cap \mathbb{Z}e_1.$$

So either

$$k = k_2 f_2$$

or

$$k = k_1 f_1 + k_2 f_2$$

for some $k_1 \in \mathbb{Z}$. Hence these vectors span K. Now check linear independence. In the one-vector case, it is immediate. In the two-vector case, let

$$f_1 = (a, 0), \qquad f_2 = (y_1, d).$$

Suppose

$$a_1 f_1 + a_2 f_2 = (0, 0).$$

Then

$$(a_1 a + a_2 y_1,\ a_2 d) = (0, 0).$$

Since $d \neq 0$, we get

$$a_2 = 0.$$

Then

$$a_1 a = 0,$$

and since $a \neq 0$, we get

$$a_1 = 0.$$

So the vectors are linearly independent. Therefore they form a basis. □

10.2 Group Actions

Let G be a finite group and let A be a set. We say G acts on A if there is a homomorphism

$$G \to \mathrm{sym}(A).$$

[10.2.0.1] Definition (*Left Translation Group Action*). A left group action of G on A is a rule assigning to each $g \in G$ and $a \in A$ an element

$$g \cdot a \in A$$

such that

$$1 \cdot a = a$$

and

$$(gh) \cdot a = g \cdot (h \cdot a).$$

The most general example is the action of G on itself by left translation, also called the Cayley action, where

$$g \mapsto \varphi_g, \qquad \varphi_g(x) = gx.$$

[10.2.0.2] Definition (*Right Conjugation Action*). A right action of G on A is a rule assigning to each $g \in G$ and $a \in A$ an element

$$a^g \in A$$

such that

$$a^1 = a$$

and

$$a^{gh} = (a^g)^h.$$

[10.2.0.3] Definition (*Left Conjugation Action*). A left action of G on A may also be written as

$$^g a$$

for $g \in G$ and $a \in A$, such that

$$^1 a = a$$

and

$$^{gh} a = {}^g({}^h a).$$

[10.2.0.4] Definition (*Orbit*). Suppose G acts on A by left translation. Let $a \in A$. Then the orbit of a under the action is

$$\{g \cdot a : g \in G\} =: \mathcal{O}(a).$$

[10.2.0.5] Lemma. For the Cayley action of G on itself, the orbit of any element is all of G.

$\therefore$

Proof. Let $a \in G$. Then

$$\mathcal{O}(a) = \{ga : g \in G\}.$$

Given any $x \in G$, choose

$$g = xa^{-1}.$$

Then

$$g \cdot a = (xa^{-1})a = x.$$

So every element of G lies in the orbit of a. Hence

$$\mathcal{O}(a) = G.$$

□

If the action is written on the right, then

$$\mathcal{O}(a) = \{a^g : g \in G\}.$$

If G acts on itself by conjugation, then

$$\mathcal{O}(x) = \{gxg^{-1} : g \in G\},$$

which is the conjugacy class of x. We denote this by $\mathcal{C}_x$. If G is abelian, then

$$\mathcal{C}_x = \{x\}$$

for every $x \in G$.

[10.2.0.6] Example. If

$$G = S_3,$$

then

$$\mathcal{C}_{(12)} = \{(12), (13), (23)\}.$$

Also,

$$G = \mathcal{C}_1 \sqcup \mathcal{C}_{(12)} \sqcup \mathcal{C}_{(123)}.$$

If G acts on A, then we can define a relation on A by declaring

$$a \sim b$$

if a and b are in the same orbit. This is an equivalence relation.

[10.2.0.7] Definition (*Stabilizer*). Suppose G acts on A. Let $a \in A$. Then the stabilizer of a under the action is

$$_G(a) := \{g \in G : g \cdot a = a\}$$

for a left action, and

$$_G(a) := \{g \in G : a^g = a\}$$

for a right action.

If G acts on itself by conjugation, then the stabilizer of x is exactly the centralizer

$$C_G(x).$$

[10.2.0.8] Theorem (*Orbit-Stabilizer Theorem*). Suppose G acts on a set A and let $a \in A$. Then:

1. $_G(a) \leq G$;
2. $$[G :_G (a)] = \text{ord}(\mathcal{O}(a)).$$

Proof. **(1)** Let $H =_G (a)$. Since
$$1 \cdot a = a,$$
we have
$$1 \in H.$$
If $g, h \in H$, then
$$h \cdot a = a.$$
So
$$(gh) \cdot a = g \cdot (h \cdot a) = g \cdot a = a.$$
Hence
$$gh \in H.$$
Now if $g \in H$, then
$$g \cdot a = a.$$
Apply g^{-1} to both sides:
$$g^{-1} \cdot (g \cdot a) = g^{-1} \cdot a.$$
Thus
$$a = g^{-1} \cdot a,$$
so
$$g^{-1} \in H.$$
Therefore
$$H \leq G.$$

(2) We find a bijection between the set of left cosets of H in G and the orbit of a. Define
$$gH \longmapsto g \cdot a.$$
We need to check that this is well-defined. Now
$$g_1 H = g_2 H \iff g_2^{-1} g_1 \in H \iff (g_2^{-1} g_1) \cdot a = a.$$
This is equivalent to
$$g_1 \cdot a = g_2 \cdot a.$$
So the map is well-defined and injective. It is surjective by definition of the orbit. Hence
$$[G : H] = \text{ord}(\mathcal{O}(a)).$$
That is,
$$[G :_G (a)] = \text{ord}(\mathcal{O}(a)).$$

□

[10.2.0.9] Definition (*Class Equation*). Let G act on itself by conjugation. Then G is the union of its disjoint conjugacy classes. Suppose these have representatives

$$z_1 = 1, z_2, \ldots, z_k, x_1, x_2, \ldots, x_r,$$

where the z_i are the elements of the center $Z(G)$, so their conjugacy classes have size 1. Then the class equation for G is

$$\operatorname{ord}(G) = \operatorname{ord}(Z(G)) + \operatorname{ord}(\mathcal{C}_{x_1}) + \cdots + \operatorname{ord}(\mathcal{C}_{x_r}).$$

Using orbit-stabilizer, this may also be written as

$$\operatorname{ord}(G) = \operatorname{ord}(Z(G)) + \sum_{i=1}^{r} [G : C_G(x_i)].$$

[10.2.0.10] Example. Suppose P is a group with

$$\operatorname{ord}(P) = p^n,$$

where p is prime. Then

$$Z(P) \neq \{1\}.$$

Proof. From the class equation,

$$\operatorname{ord}(P) = \operatorname{ord}(Z(P)) + \sum_{i=1}^{r} [P : C_P(x_i)].$$

Now for each $x_i \notin Z(P)$,

$$[P : C_P(x_i)] = \frac{p^n}{\operatorname{ord}(C_P(x_i))}.$$

Since $C_P(x_i)$ is a proper subgroup of P, its order is p^m for some $m < n$. Thus

$$[P : C_P(x_i)] = p^{n-m},$$

which is divisible by p. Therefore every term in the sum

$$\sum_{i=1}^{r} [P : C_P(x_i)]$$

is divisible by p. Since $\operatorname{ord}(P) = p^n$ is also divisible by p, it follows that

$$\operatorname{ord}(Z(P))$$

is divisible by p. Hence

$$\operatorname{ord}(Z(P)) \neq 1.$$

So

$$Z(P) \neq \{1\}.$$

■

10.3 Sylow Theorems

[10.3.0.1] Theorem (*First Sylow Theorem*). Suppose $\text{ord}(G) < \infty$ and $p \mid \text{ord}(G)$. If p^n is the highest power of p dividing $\text{ord}(G)$, then there exists a subgroup

$$P \leq G$$

such that

$$\text{ord}(P) = p^n.$$

Such a subgroup is called a Sylow-p subgroup.

$\therefore$

Proof. □

[10.3.0.2] Example. Let

$$G = S_4.$$

Then

$$\text{ord}(S_4) = 24 = 2^3 \cdot 3.$$

By the First Sylow Theorem, there exists a subgroup $P \leq S_4$ with

$$\text{ord}(P) = 8$$

for $p = 2$, and there exists a subgroup $Q \leq S_4$ with

$$\text{ord}(Q) = 3$$

for $p = 3$.

[10.3.0.3] Example. Let

$$G = S_4.$$

Then

$$Z(G) = \{e\}.$$

The possible cycle structures in S_4 are given by the partitions of 4:

$$\begin{aligned} 4 = 4 &\implies (1234), \\ 4 = 3 + 1 &\implies (123)(4), \\ 4 = 2 + 2 &\implies (12)(34), \\ 4 = 2 + 1 + 1 &\implies (12)(3)(4), \\ 4 = 1 + 1 + 1 + 1 &\implies (1)(2)(3)(4). \end{aligned}$$

How many distinct conjugacy classes are there. We need to keep in mind that two permutations with the same cycle structure lie in the same conjugacy class.

Proof. The sizes of the conjugacy classes are:

$$\begin{aligned} 4 &\implies \frac{4!}{4} = 6, \\ 3+1 &\implies \binom{4}{3}\frac{3!}{3} = 4 \cdot 2 = 8, \\ 2+2 &\implies \frac{\binom{4}{2}}{2} = 3, \\ 2+1+1 &\implies \binom{4}{2} = 6, \\ 1+1+1+1 &\implies 1. \end{aligned}$$

These add up to

$$6+8+3+6+1 = 24.$$

The last term corresponds to the center, and the others are the noncentral conjugacy classes. ■

[10.3.0.4] THEOREM (*Cauchy's Theorem*). If $p \mid \mathrm{ord}(G)$, then G has an element of order p. Hence G has a subgroup of order p.

∴

Proof. We prove this by induction on $\mathrm{ord}(G)$. Let $1 \neq a \in G$. If

$$p \mid \mathrm{ord}(a),$$

then

$$a^{\mathrm{ord}(a)/p}$$

has order p, so we are done. Suppose instead that

$$p \nmid \mathrm{ord}(a).$$

Then

$$p \mid \frac{\mathrm{ord}(G)}{\mathrm{ord}(\langle a \rangle)} = \mathrm{ord}(G/\langle a \rangle)$$

in the sense that p divides the index $[G : \langle a \rangle]$. By induction applied to a suitable smaller subgroup arising from this situation, one obtains an element of order p. Thus G has an element of order p, and therefore a subgroup of order p. □

[10.3.0.5] EXAMPLE. If

$$G = S_4,$$

then the class equation is

$$24 = 1+8+3+6+6.$$

This corresponds to the classes represented by

$$(1),\ (123),\ (12)(34),\ (12),\ (1234).$$

[10.3.0.6] THEOREM. If $\text{ord}(G) < \infty$ and $p^n \,||\, \text{ord}(G)$, then G has a subgroup of order p^n.

$\therefore$

Proof. We prove this by induction on $\text{ord}(G)$. **Case 1.** Suppose

$$p \mid \text{ord}(Z(G)).$$

Then by Cauchy's Theorem, $Z(G)$ has a subgroup N of order p. Since $N \leq Z(G)$, it follows that

$$N \trianglelefteq G.$$

Consider

$$\overline{G} = G/N.$$

Then

$$\text{ord}(\overline{G}) = \frac{\text{ord}(G)}{p},$$

so

$$p^{n-1} \,||\, \text{ord}(\overline{G}).$$

By the induction hypothesis, $\overline{G}$ contains a subgroup T of order p^{n-1}. By the correspondence theorem, T lifts to a subgroup $H \leq G$ containing N such that

$$\text{ord}(H) = \text{ord}(N)\text{ord}(T) = p \cdot p^{n-1} = p^n.$$

Case 2. Suppose

$$p \nmid \text{ord}(Z(G)).$$

From the class equation,

$$\text{ord}(G) = \text{ord}(Z(G)) + \sum_{i=1}^{r} [G : C_G(x_i)].$$

Since $p \mid \text{ord}(G)$ but $p \nmid \text{ord}(Z(G))$, there must exist some i such that

$$p \nmid [G : C_G(x_i)].$$

Now

$$\text{ord}(G) = \text{ord}(C_G(x_i))[G : C_G(x_i)].$$

Since $p^n \,||\, \text{ord}(G)$ and $p \nmid [G : C_G(x_i)]$, it follows that

$$p^n \,||\, \text{ord}(C_G(x_i)).$$

Also,

$$\text{ord}(C_G(x_i)) < \text{ord}(G).$$

By the induction hypothesis, $C_G(x_i)$ has a subgroup P of order p^n. Since

$$P \leq C_G(x_i) \leq G,$$

this is also a subgroup of G of order p^n. □

[10.3.0.7] THEOREM (*Second Sylow Theorem*). All Sylow-p subgroups are conjugate in G. That is, if $P, Q \leq G$ are Sylow-p subgroups, then there exists $g \in G$ such that

$$Q = P^g = gPg^{-1} = \{gxg^{-1} : x \in P\}.$$

∴

Proof. □

[10.3.0.8] Theorem (*Third Sylow Theorem*). The number of Sylow-p subgroups of G is congruent to $1 \mod p$ and is equal to

$$[G : N_G(P)],$$

where P is any Sylow-p subgroup and

$$N_G(P) := \{g \in G : gPg^{-1} = P\}.$$

In particular, the number of Sylow-p subgroups divides

$$[G : P].$$

∴

Proof. Let P be a Sylow-p subgroup. Let

$$S := \{P^g : g \in G\},$$

the set of all conjugates of P. Then G acts on S by conjugation. The orbit of P under this action is all of S. The stabilizer of P is

$$_G(P) = \{g \in G : P^g = P\} = N_G(P).$$

So by orbit-stabilizer,

$$\text{ord}(S) = [G : N_G(P)].$$

Thus the number of Sylow-p subgroups is

$$[G : N_G(P)].$$

Now let Q be any Sylow-p subgroup. Then Q acts on S by conjugation. The size of each orbit under this action is a power of p. Since $\text{ord}(S) = [G : N_G(P)]$ is not divisible by p, at least one orbit has size 1. So there exists some $T \in S$ fixed by all elements of Q. This means

$$Q \leq N_G(T).$$

Since T is a Sylow-p subgroup and Q is also a Sylow-p subgroup, it follows that

$$Q = T.$$

Thus every Sylow-p subgroup is conjugate to P. Finally, since the Q-orbits on S have sizes powers of p, and exactly one of them has size 1, the total number satisfies

$$\text{ord}(S) \equiv 1 \mod p.$$

So the number of Sylow-p subgroups is congruent to $1 \mod p$. □

[10.3.0.9] Lemma. If Q and T are both Sylow-p subgroups, then

$$_Q(T) = Q \quad \text{if and only if} \quad Q = T.$$

$\therefore$

Proof. Now

$$_Q(T) = Q \cap N_G(T).$$

If $_Q(T) = Q$, then

$$Q \leq N_G(T).$$

Hence

$$QT$$

is a subgroup of $N_G(T)$, and $T \trianglelefteq QT$. By the second isomorphism theorem,

$$QT/T \cong Q/(Q \cap T).$$

Since Q and T are Sylow-p subgroups, the quotient on the right is a p-group. But the order of QT/T must divide the index of T in its normalizer, which is not divisible by p. Therefore

$$QT/T$$

is trivial, so

$$Q \leq T.$$

Since both have the same order,

$$Q = T.$$

Conversely, if

$$Q = T,$$

then every element of Q stabilizes T under conjugation, so

$$_Q(T) = Q.$$

□

[10.3.0.10] THEOREM. Suppose

$$\text{ord}(G) = 2q$$

where q is an odd prime, and suppose G is not abelian. Then

$$G \cong H \leq S_q,$$

where H is generated by a q-cycle and an element of order 2.

$\therefore$

Proof. Given

$$\text{ord}(G) = 2q,$$

G has a Sylow-2 subgroup, say

$$P_i = \langle x_i \rangle$$

with $\text{ord}(x_i) = 2$. The number of Sylow-2 subgroups divides

$$\frac{\text{ord}(G)}{2} = q$$

and is congruent to $1 \mod 2$. Since G is not abelian, this number is not 1, so it must be q.

Thus there are q distinct Sylow-2 subgroups

$$P_1 = \langle x_1 \rangle,\ P_2 = \langle x_2 \rangle,\ \ldots,\ P_q = \langle x_q \rangle.$$

Now define

$$\varphi : G \to \mathrm{sym}(\{x_1, \ldots, x_q\}) \cong S_q$$

by

$$\varphi(g)(x_i) = g x_i g^{-1}.$$

This is a homomorphism coming from the conjugation action. We claim that $\ker\varphi = \{1\}$. Indeed, if $y \in \ker\varphi$, then

$$y x_i y^{-1} = x_i$$

for all i, so y commutes with every x_i. If y had order 2, then together with some x_i it would generate a subgroup of order 4, impossible since $4 \nmid 2q$. So the kernel cannot contain an element of order 2. Also, the kernel cannot have order q or $2q$, since then it would force too much normality and make G abelian. Hence

$$\ker\varphi = \{1\}.$$

So φ is injective, and therefore

$$G \cong \varphi(G) \leq S_q.$$

□

[10.3.0.11] Example. Let $g \in G$ with

$$\mathrm{ord}(g) = q.$$

Let

$$x_1 = x, \quad x_2 = x_1^g, \quad x_3 = x_2^g, \quad \ldots, \quad x_q = x_{q-1}^g, \quad x_1 = x_q^g.$$

Then g acts as a q-cycle on the set $\{x_1, \ldots, x_q\}$. Thus the image of G in S_q is generated by a q-cycle and an element of order 2. So it is isomorphic to the dihedral group of order $2q$.

[10.3.0.12] Example (*Why is the kernel trivial*). Claim:

$$K = \ker\varphi = \{1\}.$$

Suppose $y \in K$ and $\mathrm{ord}(y) = 2$. Then y commutes with every x_i. So y together with some x_i would generate a subgroup isomorphic to

$$\mathbb{Z}_2 \times \mathbb{Z}_2,$$

which has order 4. But $4 \nmid 2q$ since q is odd. This is impossible. Hence K contains no element of order 2. A similar order argument rules out the possibilities $\mathrm{ord}(K) = q$ and $\mathrm{ord}(K) = 2q$. Therefore

$$K = \{1\}.$$

Chapter 11

Galois Theory

11.1 Field Extensions

Refer to Chapter 7.2 for all the theory on field extensions. We will be continuing this on behalf of learning Galois Theory.

[11.1.0.1] Definition. Given $u \in \mathbb{E} \supseteq \mathbb{F}$, $\mathbb{F}(u)$ is the intersection of all subfields of $\mathbb{E}$ containing $\mathbb{F}$ and u. That is,

$$\mathbb{F}(u) := \bigcap_{\substack{\mathbb{E}_i \subseteq \mathbb{E} \\ \mathbb{F} \subseteq \mathbb{E}_i,\ u \in \mathbb{E}_i}} \mathbb{E}_i.$$

It is the smallest field extension of $\mathbb{F}$ containing u. That is, if $\mathbb{K}$ is a field with

$$\mathbb{F} \subseteq \mathbb{K} \quad \text{and} \quad u \in \mathbb{K},$$

then

$$\mathbb{F}(u) \subseteq \mathbb{K}.$$

Thus if u is algebraic over $\mathbb{F}$, then $\mathbb{F}[u]$ is a field extension of $\mathbb{F}$ with $u \in \mathbb{F}[u]$. Hence

$$\mathbb{F}(u) \subseteq \mathbb{F}[u].$$

Let $f(u) \in \mathbb{F}[u]$, where $f(x) \in \mathbb{F}[x]$. Then it is always true that $f(u) \in \mathbb{F}(u)$, since $\mathbb{F}(u)$ must contain every polynomial in u. Thus

$$\mathbb{F}[u] \subseteq \mathbb{F}(u).$$

Therefore, when u is algebraic over $\mathbb{F}$,

$$\mathbb{F}(u) = \mathbb{F}[u].$$

Let $f(x) \in \mathbb{F}[x]$. If $p(x)$ is an irreducible factor of $f(x)$, then

$$\frac{\mathbb{F}[x]}{(p(x))}$$

is a field containing $\mathbb{F}$, really a copy consisting of classes of constant polynomials. It also has a root of $p(x)$, namely the class of x. For example, if

$$f(x) = x^2 - 2$$

in $\mathbb{Q}[x]$, then

$$\mathbb{Q}\left[\sqrt{2}\right] \cong \frac{\mathbb{Q}[x]}{(x^2-2)}.$$

Thus $\sqrt{2}$ corresponds to the class of x. The map

$$\mathbb{Q}[x] \to \mathbb{Q}\left[\sqrt{2}\right]$$

is defined by

$$f(x) \mapsto f\left(\sqrt{2}\right),$$

so

$$x \mapsto \sqrt{2}.$$

Then $p(\alpha)$ is equal to the class of $p(x)$. But since we mod out by $(p(x))$, that is equal to

$$0 \in \frac{\mathbb{F}[x]}{(p(x))}.$$

[11.1.0.2] THEOREM. Let $p(x) \in \mathbb{F}_1[x]$ be irreducible. Let

$$\mathbb{K}_1 := \frac{\mathbb{F}_1[x]}{(p(x))}.$$

Then $\mathbb{K}_1$ is a field extension of $\mathbb{F}_1$ in which $p(x)$ has a root $\alpha \in \mathbb{K}_1$, where α is the class of x. Suppose

$$\sigma : \mathbb{F}_1 \to \mathbb{F}_2$$

is a field isomorphism. If

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}_1[x],$$

define

$$\sigma f(x) := \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n \in \mathbb{F}_2[x].$$

Then irreducibility is preserved. That is, if $p(x)$ is irreducible in $\mathbb{F}_1[x]$, then $\sigma p(x)$ is irreducible in $\mathbb{F}_2[x]$. Let $u \in \mathbb{E}_1$ be a root of $p(x)$. Suppose v is a root of $\sigma p(x) \in \mathbb{F}_2[x]$. Then there exists an isomorphism

$$\overline{\sigma} : \mathbb{F}_1(u) \to \mathbb{F}_2(v)$$

extending σ, such that

$$\overline{\sigma}|_{\mathbb{F}_1} = \sigma \quad \text{and} \quad \overline{\sigma}(u) = v.$$

Proof.

$$\mathbb{F}_1(u) \cong \frac{\mathbb{F}_1[x]}{(p(x))} \cong \frac{\mathbb{F}_2[x]}{(\sigma p(x))} \cong \mathbb{F}_2(v).$$

The first and third isomorphisms come from evaluation at u and v, respectively. The middle isomorphism is induced by σ on coefficients. Under these identifications, the class of x in

$$\frac{\mathbb{F}_1[x]}{(p(x))}$$

corresponds to the class of x in

$$\frac{\mathbb{F}_2[x]}{(\sigma p(x))}$$

and hence to v. Thus we obtain an isomorphism

$$\overline{\sigma} : \mathbb{F}_1(u) \to \mathbb{F}_2(v)$$

such that

$$\overline{\sigma}(u) = v.$$

Also,

$$\overline{\sigma}(1_{\mathbb{F}_1}) = 1_{\mathbb{F}_2}.$$

So $\overline{\sigma}$ is an extension of σ. □

[11.1.0.3] Corollary. The number of such extensions is at most the number of distinct roots of $\sigma p(x)$ in a chosen overfield containing $\mathbb{F}_2(v)$.

∴

Proof. □

[11.1.0.4] Definition (*Splitting Field*). A splitting field for $f(x) \in \mathbb{F}[x]$ is an extension field $\mathbb{E}$ of $\mathbb{F}$ such that in $\mathbb{E}[x]$ we have

$$f(x) = c(x - a_1) \cdots (x - a_n), \qquad a_i \in \mathbb{E},$$

and

$$\mathbb{E} = \mathbb{F}(a_1, \ldots, a_n).$$

[11.1.0.5] Theorem. There exists a splitting field for every polynomial $f(x) \in \mathbb{F}[x]$.

∴

Proof. We prove this by induction on $\deg(f)$. If $\deg(f) = 1$, then f is already linear, so $\mathbb{F}$ itself is a splitting field. Now assume $\deg(f) > 1$. Choose an irreducible factor $p(x)$ of $f(x)$. Then

$$\mathbb{E}_1 := \frac{\mathbb{F}[x]}{(p(x))}$$

is a field extension of $\mathbb{F}$ in which $p(x)$ has a root u. Hence in $\mathbb{E}_1[x]$,

$$f(x) = (x - u)g(x)$$

for some $g(x)$ with

$$\deg(g) < \deg(f).$$

By the induction hypothesis, there exists a splitting field $\mathbb{E}$ for $g(x)$ over $\mathbb{E}_1$. Then $\mathbb{E}$ is a splitting field for $f(x)$ over $\mathbb{F}$. □

[11.1.0.6] Theorem. Any two splitting fields for $f(x)$ over $\mathbb{F}$ are isomorphic over $\mathbb{F}$.

∴

Proof. Suppose

$$\sigma : \mathbb{F}_1 \xrightarrow{\sim} \mathbb{F}_2$$

is a field isomorphism. Let $f(x) \in \mathbb{F}_1[x]$. Suppose $\mathbb{E}_1$ is a splitting field for $f(x)$ over $\mathbb{F}_1$, and $\mathbb{E}_2$ is a splitting field for $\sigma f(x)$ over $\mathbb{F}_2$. We prove by induction on

$$[\mathbb{E}_1 : \mathbb{F}_1]$$

that σ extends to an isomorphism

$$\overline{\sigma} : \mathbb{E}_1 \to \mathbb{E}_2.$$

If

$$[\mathbb{E}_1 : \mathbb{F}_1] = 1,$$

then $\mathbb{E}_1 = \mathbb{F}_1$, and the result is immediate. Assume now

$$[\mathbb{E}_1 : \mathbb{F}_1] > 1.$$

Let $p(x)$ be an irreducible factor of $f(x)$, and let $r \in \mathbb{E}_1$ be a root of $p(x)$. If v is any root of $\sigma p(x)$ in $\mathbb{E}_2$, then by the previous theorem there exists an extension

$$\sigma_1 : \mathbb{F}_1(r) \xrightarrow{\sim} \mathbb{F}_2(v).$$

Now $\mathbb{E}_1$ is a splitting field of $f(x)$ over $\mathbb{F}_1(r)$, and $\mathbb{E}_2$ is a splitting field of $\sigma_1 f(x)$ over $\mathbb{F}_2(v)$. Since

$$[\mathbb{E}_1 : \mathbb{F}_1(r)] < [\mathbb{E}_1 : \mathbb{F}_1],$$

the induction hypothesis applies. Thus σ_1 extends to an isomorphism

$$\overline{\sigma} : \mathbb{E}_1 \to \mathbb{E}_2.$$

In particular, if

$$\mathbb{F}_1 = \mathbb{F}_2 = \mathbb{F}$$

and $\sigma = \mathrm{id}_{\mathbb{F}}$, then any two splitting fields of $f(x)$ over $\mathbb{F}$ are isomorphic over $\mathbb{F}$. Thus splitting fields are unique up to isomorphism. □

11.2 Galois Theory

Define a homomorphism

$$\varphi : \mathbb{Z} \to \mathbb{F}$$

by

$$1 \mapsto 1$$

and hence

$$n \mapsto n1.$$

Then

$$\varphi(n+m) = \varphi(n) + \varphi(m)$$

and

$$\varphi(nm) = \varphi(n)\varphi(m).$$

Thus $\mathrm{Im}(\varphi)$ is a subring of $\mathbb{F}$. Also,

$$\frac{\mathbb{Z}}{\ker \varphi} \cong \mathrm{Im}(\varphi).$$

Since $\ker\varphi$ is an ideal of $\mathbb{Z}$, it has the form

$$n\mathbb{Z}$$

for some $n \geq 0$. If

$$\ker\varphi = \{0\},$$

then $\mathbb{F}$ contains a subring isomorphic to $\mathbb{Z}$, hence a subfield isomorphic to $\mathbb{Q}$. We say in this case that $\mathbb{F}$ has characteristic 0. If

$$\ker\varphi = p\mathbb{Z}$$

for some prime p, then

$$\mathbb{F}$$

contains a subfield isomorphic to

$$\mathbb{Z}_p \cong \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

We then say that $\mathbb{F}$ has characteristic p.

[11.2.0.1] DEFINITION (*Formal Derivative*). If

$$f(x) \in \mathbb{F}[x],$$

then the formal derivative of f is denoted by

$$f'(x) = Df(x).$$

If

$$f(x) = x^n,$$

then

$$Df(x) = nx^{n-1},$$

and this extends to all of $\mathbb{F}[x]$ by linearity.

Alternatively, in $\mathbb{F}[x,h]$, where h is transcendental, define

$$g(x,h) = f(x+h) - f(x).$$

Then

$$g(x,0) = 0.$$

By the factor theorem, h divides $g(x,h)$.

[11.2.0.2] DEFINITION.

$$Df(x)$$

is the polynomial obtained from

$$\frac{g(x,h)}{h}$$

by evaluating at

$$h = 0.$$

[11.2.0.3] DEFINITION (*Repeated Root*). Let

$$f(x) \in \mathbb{F}[x],$$

and let $\mathbb{E}$ be a splitting field for $f(x)$. We say that a is a repeated root of $f(x)$ if

$$f(x) = (x-a)^2 g(x)$$

in $\mathbb{E}[x]$ for some $g(x) \in \mathbb{E}[x]$.

If a is a repeated root of $f(x)$, then

$$f(a) = 0 \quad \text{and} \quad Df(a) = 0.$$

So a is a common root of $f(x)$ and $Df(x)$. Now assume $\mathbb{E}$ is a finite-dimensional extension of $\mathbb{Q}$. Then $\text{char}(\mathbb{E}) = 0$. Let $\mathbb{F}$ be a subfield of $\mathbb{E}$. If

$$f(x) \in \mathbb{F}[x]$$

is irreducible and $u \in \mathbb{E}$ is a root of $f(x)$, then u is not a repeated root of $f(x)$. Indeed, if u were a repeated root, then

$$Df(u) = 0.$$

Since

$$\deg(Df) < \deg(f),$$

this would contradict the minimality of the irreducible polynomial $f(x)$.

[11.2.0.4] DEFINITION (*Normal Extension*). Suppose $\mathbb{E}/\mathbb{F}$ is a field extension. We say $\mathbb{E}$ is normal over $\mathbb{F}$ if whenever

$$u \in \mathbb{E}$$

and $f(x) \in \mathbb{F}[x]$ is the minimal polynomial of u over $\mathbb{F}$, then $f(x)$ splits completely in $\mathbb{E}[x]$.

Equivalently, any polynomial in $\mathbb{F}[x]$ which has one root in $\mathbb{E}$ has all of its roots in $\mathbb{E}$.

[11.2.0.5] EXAMPLE. If $\mathbb{E}$ is a splitting field for

$$f(x) \in \mathbb{F}[x],$$

then $\mathbb{E}$ is normal over $\mathbb{F}$. For example, let

$$\omega = e^{2\pi i/3}.$$

Then

$$\mathbb{Q}\left(2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2\right) = \mathbb{Q}\left(2^{1/3}, \omega\right)$$

is the splitting field for

$$x^3 - 2$$

over $\mathbb{Q}$, so it is normal over $\mathbb{Q}$. But

$$\mathbb{Q}\left(2^{1/3}\right)$$

is not normal over $\mathbb{Q}$.

[11.2.0.6] Definition (*Automorphism*).

$$\mathrm{Aut}(\mathbb{E})$$

is the group of field automorphisms of $\mathbb{E}$.

[11.2.0.7] Definition (*Galois Group*).

$$\mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right) := \{\sigma \in \mathrm{Aut}(\mathbb{E}) : \sigma(a) = a \ \forall a \in \mathbb{F}\} = \mathrm{Gal}\left(\frac{\mathbb{E}}{\mathbb{F}}\right).$$

[11.2.0.8] Definition (*Fixed Field*). Let

$$G = \mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right).$$

The fixed field of G is

$$\{u \in \mathbb{E} : \sigma(u) = u \ \forall \sigma \in G\} = \mathrm{Inv}(G).$$

Note that

$$\mathbb{F} \subseteq \mathrm{Inv}(G),$$

but it is not automatic that $\mathrm{Inv}(G) = \mathbb{F}$.

[11.2.0.9] Example. Let

$$\mathbb{F} = \mathbb{Q}, \qquad \mathbb{E} = \mathbb{Q}(2^{1/3}).$$

Then

$$G = \mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right) = \{1\}.$$

So

$$\mathrm{Inv}(G) = \mathbb{E},$$

which is strictly larger than $\mathbb{F}$.

[11.2.0.10] Theorem (*Fundamental Theorem of Galois Theory*). Assume

$$[\mathbb{E} : \mathbb{F}] < \infty$$

and

$$\mathrm{char}(\mathbb{F}) = 0.$$

Then the following are equivalent:

1.
$$\mathrm{Inv}\left(\mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right)\right) = \mathbb{F};$$

2.
$$\mathbb{F} = \mathrm{Inv}(G)$$

for some finite subgroup

$$G \leq \mathrm{Aut}(\mathbb{E});$$

3. $\mathbb{E}$ is normal over $\mathbb{F}$;
4. $\mathbb{E}$ is the splitting field of a separable polynomial in $\mathbb{F}[x]$;
5. $$\mathrm{ord}\left(\mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right)\right) = [\mathbb{E} : \mathbb{F}].$$

Proof. We sketch the main implications.

$$(\mathbf{4}) \implies (\mathbf{5})$$

has already been shown.

$$(\mathbf{1}) \implies (\mathbf{2})$$

is immediate by taking

$$G = \mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right).$$

$$(\mathbf{3}) \implies (\mathbf{4}).$$

Since

$$[\mathbb{E} : \mathbb{F}] < \infty,$$

we can write

$$\mathbb{E} = \mathbb{F}(u_1, \ldots, u_n).$$

Let

$$p_i(x) \in \mathbb{F}[x]$$

be the minimal polynomial of u_i over $\mathbb{F}$. Because $\mathbb{E}/\mathbb{F}$ is normal, each $p_i(x)$ splits in $\mathbb{E}[x]$. Let $f(x)$ be the product of the distinct $p_i(x)$. Then $\mathbb{E}$ is the splitting field of $f(x)$ over $\mathbb{F}$. Since $\mathrm{char}(\mathbb{F}) = 0$, the polynomial is separable.

$$(\mathbf{2}) \implies (\mathbf{3}).$$

Assume

$$\mathbb{F} = \mathrm{Inv}(G)$$

for some finite subgroup

$$G \leq \mathrm{Aut}(\mathbb{E}).$$

Let $u \in \mathbb{E}$. Consider its orbit under G:

$$u_1 = u,\ u_2, \ldots, u_m.$$

Define

$$g(x) = (x - u_1) \cdots (x - u_m) \in \mathbb{E}[x].$$

We claim that

$$g(x) \in \mathbb{F}[x].$$

Indeed, each $\sigma \in G$ permutes the roots u_i, so it fixes the coefficients of $g(x)$. Hence the coefficients lie in $\mathrm{Inv}(G) = \mathbb{F}$. Thus the minimal polynomial of u over $\mathbb{F}$ divides $g(x)$ and therefore splits in $\mathbb{E}[x]$. So $\mathbb{E}/\mathbb{F}$ is normal. Since $\mathrm{char}(\mathbb{F}) = 0$, it is also separable.

$$(\mathbf{5}) \implies (\mathbf{1}).$$

Let

$$\mathbb{K} = \mathrm{Inv}\left(\mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right)\right).$$

Then by construction

$$\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}.$$

Also,

$$\mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{K}}\right) = \mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right).$$

By Artin's theorem and condition (**5**),

$$[\mathbb{E} : \mathbb{K}] = \mathrm{ord}\left(\mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{K}}\right)\right) = \mathrm{ord}\left(\mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right)\right) = [\mathbb{E} : \mathbb{F}].$$

Hence

$$\mathbb{K} = \mathbb{F}.$$

So condition (**1**) holds. □

[11.2.0.11] LEMMA. Let $\mathbb{E}$ be an extension field of $\mathbb{F}$. Let

$$G = \mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right)$$

and let

$$\mathbb{K} = \mathrm{Inv}(G).$$

Then

$$\mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{K}}\right) = \mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right) = G.$$

∴

Proof. This is immediate from the definition of fixed field. An automorphism fixes $\mathbb{F}$ if and only if it fixes every element fixed by all elements of G. □

[11.2.0.12] DEFINITION (*Galois*). We say

$$\frac{\mathbb{E}}{\mathbb{F}}$$

is Galois if any of the equivalent conditions above hold.

[11.2.0.13] THEOREM. If

$$G \leq \mathrm{Aut}(\mathbb{E})$$

is finite and

$$\mathbb{K} = \mathrm{Inv}(G),$$

then

$$[\mathbb{E} : \mathbb{K}] \leq \mathrm{ord}(G).$$

Proof. This is Artin's Lemma. Suppose, for contradiction, that there exist

$$u_1, \ldots, u_m \in \mathbb{E}$$

which are linearly independent over $\mathbb{K}$ with

$$m > \mathrm{ord}(G) = n.$$

Write

$$G = \{\sigma_1, \ldots, \sigma_n\},$$

where $\sigma_1 = 1$. Form the matrix

$$A = \begin{bmatrix} \sigma_1(u_1) & \sigma_1(u_2) & \cdots & \sigma_1(u_m) \\ \sigma_2(u_1) & \sigma_2(u_2) & \cdots & \sigma_2(u_m) \\ \vdots & \vdots & & \vdots \\ \sigma_n(u_1) & \sigma_n(u_2) & \cdots & \sigma_n(u_m) \end{bmatrix}.$$

This is an $n \times m$ matrix with $m > n$, so the system

$$A\vec{x} = \vec{0}$$

has a nontrivial solution. Choose a nontrivial solution

$$\vec{b} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

with the fewest number of nonzero entries. After scaling and reordering, we may assume

$$b_1 = 1.$$

We claim that each

$$b_i \in \mathbb{K}.$$

Suppose not. Then there exists some $\sigma_\ell \in G$ such that

$$\sigma_\ell(b_j) \neq b_j$$

for some j. Applying σ_ℓ to the equation

$$A\vec{b} = \vec{0}$$

shows that

$$\sigma_\ell(\vec{b})$$

is also a solution. Hence

$$\vec{b} - \sigma_\ell(\vec{b})$$

is a nontrivial solution with fewer nonzero entries, contradicting minimality. Thus

$$\vec{b} \in \mathbb{K}^m.$$

So we have found a nontrivial linear relation among

$$u_1, \dots, u_m$$

with coefficients in $\mathbb{K}$, contradicting linear independence. Therefore

$$[\mathbb{E} : \mathbb{K}] \leq \operatorname{ord}(G).$$

□

[11.2.0.14] THEOREM. Suppose

$$\mathbb{E}/\mathbb{F}$$

is Galois, and let

$$G = \operatorname{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right).$$

Then for every intermediate field

$$\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E},$$

the extension

$$\mathbb{E}/\mathbb{K}$$

is Galois. Moreover, there is a bijection between intermediate fields $\mathbb{K}$ and subgroups

$$H \leq G.$$

The correspondence is given by

$$\mathbb{K} \longmapsto \operatorname{Aut}\left(\frac{\mathbb{E}}{\mathbb{K}}\right)$$

and

$$H \longmapsto \operatorname{Inv}(H).$$

These maps are inclusion-reversing.

∴

Proof. Since $\mathbb{E}/\mathbb{F}$ is Galois, it is the splitting field of some separable polynomial

$$f(x) \in \mathbb{F}[x].$$

Because

$$\mathbb{F} \subseteq \mathbb{K},$$

the same polynomial lies in $\mathbb{K}[x]$, and $\mathbb{E}$ is still its splitting field. Thus

$$\mathbb{E}/\mathbb{K}$$

is Galois. Now let

$$H \leq G$$

and define

$$\mathbb{K} = \operatorname{Inv}(H).$$

By Artin's Lemma,

$$[\mathbb{E} : \mathbb{K}] \leq \operatorname{ord}(H).$$

Also,

$$H \leq \mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{K}}\right).$$

Since

$$\mathbb{E}/\mathbb{K}$$

is Galois, we have

$$\mathrm{ord}\left(\mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{K}}\right)\right) = [\mathbb{E}:\mathbb{K}].$$

So

$$[\mathbb{E}:\mathbb{K}] \leq \mathrm{ord}(H) \leq \mathrm{ord}\left(\mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{K}}\right)\right) = [\mathbb{E}:\mathbb{K}].$$

Hence

$$H = \mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{K}}\right).$$

Thus the two maps are inverses. □

These maps are order-reversing under inclusion. That is,

$$\mathbb{K}_1 \subseteq \mathbb{K}_2 \implies \mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{K}_1}\right) \supseteq \mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{K}_2}\right),$$

and if

$$H_1 \subseteq H_2,$$

then

$$\mathrm{Inv}(H_1) \supseteq \mathrm{Inv}(H_2).$$

[11.2.0.15] Example (*Galois Groups Fork*). Let

$$\mathbb{F} = \mathbb{Q}$$

and

$$\mathbb{E} = \mathbb{Q}\left(2^{1/3}, \omega\right), \qquad \omega = e^{2\pi i/3}.$$

Then $\mathbb{E}$ is Galois over $\mathbb{Q}$ because it is the splitting field of

$$f(x) = x^3 - 2$$

over $\mathbb{Q}$. Also,

$$[\mathbb{Q}(\omega):\mathbb{Q}] = 2.$$

When $\mathbb{E}/\mathbb{F}$ is Galois, the intermediate fields and the subgroups of

$$G = \mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right)$$

correspond exactly:

$$\mathbb{E} \underset{\mathbb{E}=\mathrm{Inv}(1)}{\overset{\mathrm{Aut}(\mathbb{E}/\mathbb{E})}{\leftrightarrows}} 1,$$

$$\mathbb{K} \underset{\mathbb{K}=\mathrm{Inv}(H)}{\overset{\mathrm{Aut}(\mathbb{E}/\mathbb{K})}{\leftrightarrows}} H,$$

$$\mathbb{F} \underset{\mathbb{F}=\mathrm{Inv}(G)}{\overset{\mathrm{Aut}(\mathbb{E}/\mathbb{F})}{\leftrightarrows}} G.$$

These maps are inverses.

What is the degree of

$$\mathbb{Q}\left(2^{1/3}, \omega\right)?$$

We get this field from the polynomial

$$x^3 - 2,$$

which has 3 roots. Automorphisms permute the roots, so the Galois group has size at most

$$\mathrm{ord}(S_3) = 6.$$

Let

$$\mathbb{E} = \mathbb{Q}\left(2^{1/3}, \omega\right).$$

What are the automorphisms in

$$G = \mathrm{Gal}\left(\frac{\mathbb{E}}{\mathbb{Q}}\right)?$$

One such automorphism is complex conjugation. Let

$$\sigma(z) = \overline{z}.$$

Then

$$\overline{z+w} = \overline{z} + \overline{w}$$

and

$$\overline{zw} = \overline{z}\,\overline{w}.$$

Also,

$$\sigma\left(2^{1/3}\right) = 2^{1/3}$$

because

$$2^{1/3} \in \mathbb{R},$$

and

$$\sigma(\omega) = \overline{\omega} = \omega^{-1} = \omega^2.$$

Then

$$\sigma^2(\omega) = \sigma(\omega^2) = \omega,$$

so

$$\sigma^2 = 1_G.$$

Chapter 12

Problem Sets

12.1 Chapter 1

[12.1.0.1] Problem (*Induction*). Use induction to prove that if k and n are nonnegative integers, then

$$\binom{k}{k}+\binom{k+1}{k}+\cdots+\binom{k+n}{k}=\binom{k+n+1}{k+1}.$$

$\therefore$

Solution. We define

$$S:=\left\{n\in\mathbb{Z}^{\geq 0}:\sum_{j=0}^{n}\binom{k+j}{k}=\binom{k+n+1}{k+1}\right\}.$$

First, $0\in S$. We can check this by substituting $n=0$ into the statement:

$$\sum_{j=0}^{0}\binom{k+j}{k}=\binom{k}{k}=\binom{k+1}{k+1}=\binom{k+1}{k}.$$

So the statement is true when $n=0$. Now suppose $n\in S$. Then

$$\sum_{j=0}^{n}\binom{k+j}{k}=\binom{k+n+1}{k+1}.$$

We must show that $(n+1)\in S$. Consider

$$\begin{aligned}\sum_{j=0}^{n+1}\binom{k+j}{k}&=\sum_{j=0}^{n}\binom{k+j}{k}+\binom{k+n+1}{k}\\&=\binom{k+n+1}{k+1}+\binom{k+n+1}{k}.\end{aligned}$$

Using Pascal's identity,

$$\binom{m}{r+1}+\binom{m}{r}=\binom{m+1}{r+1},$$

with $m=k+n+1$ and $r=k$, we get

$$\binom{k+n+1}{k+1}+\binom{k+n+1}{k}=\binom{k+n+2}{k+1}.$$

Hence

$$\sum_{j=0}^{n+1}\binom{k+j}{k}=\binom{k+n+2}{k+1}.$$

Thus $(n+1)\in S$. Therefore, by the Principle of Mathematical Induction,

$$S=\mathbb{Z}^{\geq 0}.$$

So for all nonnegative integers n,

$$\binom{k}{k}+\binom{k+1}{k}+\cdots+\binom{k+n}{k}=\binom{k+n+1}{k+1}.$$

□

12.2 Chapter 2

[12.2.0.1] Problem. Suppose $\gcd(a,b)=1$. If $a\mid c$ and $b\mid c$, prove that $ab\mid c$.

∴

Solution. Since

$$\gcd(a,b)=1,$$

there exist $x,y\in\mathbb{Z}$ such that

$$1=ax+by.$$

Now multiply both sides by c. Then

$$c=acx+bcy.$$

Since $a\mid c$ and $b\mid c$, there exist $m,n\in\mathbb{Z}$ such that

$$c=am \qquad \text{and} \qquad c=bn.$$

Substitute these into the previous equation:

$$\begin{aligned} c &= a(bn)x+b(am)y \\ &= ab(nx+my). \end{aligned}$$

Let

$$t\coloneqq nx+my\in\mathbb{Z}.$$

Then

$$c = abt.$$

Hence

$$ab \mid c.$$

□

[12.2.0.2] Problem. If $\gcd(a,c) = 1$ and $\gcd(b,c) = 1$, prove that $\gcd(ab,c) = 1$.

∴

Solution. Since

$$\gcd(a,c) = 1,$$

there exist $x, y \in \mathbb{Z}$ such that

$$1 = ax + cy.$$

Since

$$\gcd(b,c) = 1,$$

there exist $m, n \in \mathbb{Z}$ such that

$$1 = bm + cn.$$

Multiply the first equation by b:

$$b = abx + bcy.$$

Now multiply the second equation by cy:

$$cy = b(cmy) + c^2ny.$$

Substitute the expression

$$b = abx + bcy$$

into

$$1 = bm + cn:$$

$$\begin{aligned} 1 &= (abx + bcy)m + cn \\ &= ab(mx) + c(bym + n). \end{aligned}$$

Let

$$p := mx \qquad \text{and} \qquad q := bym + n.$$

Then

$$1 = abp + cq.$$

Therefore

$$\gcd(ab,c) = 1.$$

□

[12.2.0.3] Problem. (a) If $a, b, u, v \in \mathbb{Z}$ are such that $au + bv = 1$, prove that $\gcd(a,b) = 1$.

(b) Show by example that if $au + bv = d > 1$, then $\gcd(a,b)$ may not be d.

∴

Solution. **(a).** Assume

$$au + bv = 1.$$

Let $d = \gcd(a, b)$. Then

$$d \mid a \qquad \text{and} \qquad d \mid b.$$

So d divides every linear combination of a and b. In particular,

$$d \mid (au + bv) = 1.$$

Hence

$$d = 1.$$

Therefore

$$\gcd(a, b) = 1.$$

(b). Take

$$a = 6, \qquad b = 9, \qquad u = 2, \qquad v = -1.$$

Then

$$au + bv = 6(2) + 9(-1) = 12 - 9 = 3.$$

So here

$$au + bv = d = 3 > 1.$$

But

$$\gcd(6, 9) = 3,$$

so this still equals d. To get an example where the gcd is not d, take instead

$$a = 6, \qquad b = 9, \qquad u = 1, \qquad v = 1.$$

Then

$$au + bv = 6 + 9 = 15.$$

So

$$d = 15 > 1,$$

but

$$\gcd(6, 9) = 3 \neq 15.$$

Thus if

$$au + bv = d > 1,$$

it need not follow that

$$\gcd(a, b) = d.$$

□

[12.2.0.4] Problem. If $a \mid c$ and $b \mid c$ and $\gcd(a, b) = d$, prove that $ab \mid cd$.

∴

Solution. Let

$$\gcd(a, b) = d.$$

Then there exist $a_1, b_1 \in \mathbb{Z}$ such that

$$a = da_1 \qquad \text{and} \qquad b = db_1,$$

with

$$\gcd(a_1, b_1) = 1.$$

Since

$$a \mid c \qquad \text{and} \qquad b \mid c,$$

we have

$$da_1 \mid c \qquad \text{and} \qquad db_1 \mid c.$$

Hence

$$a_1 \mid \frac{c}{d} \qquad \text{and} \qquad b_1 \mid \frac{c}{d}.$$

Since

$$\gcd(a_1, b_1) = 1,$$

the previous problem implies

$$a_1 b_1 \mid \frac{c}{d}.$$

So there exists $t \in \mathbb{Z}$ such that

$$\frac{c}{d} = a_1 b_1 t.$$

Multiply both sides by d^2:

$$cd = d^2 a_1 b_1 t = (da_1)(db_1)t = abt.$$

Therefore

$$ab \mid cd.$$

□

[12.2.0.5] PROBLEM. If $a > 0$ and $b > 0$, prove that

$$lcm[a, b] = \frac{ab}{\gcd(a, b)}.$$

$\therefore$

Solution. Let

$$d = \gcd(a, b).$$

Then there exist $x, y \in \mathbb{Z}_{>0}$ such that

$$a = dx, \qquad b = dy,$$

and

$$\gcd(x, y) = 1.$$

We claim that

$$lcm[a, b] = dxy.$$

First, dxy is a common multiple of a and b because

$$dxy = ay = bx.$$

So

$$a \mid dxy \qquad \text{and} \qquad b \mid dxy.$$

Now let m be any common multiple of a and b. Then

$$a \mid m \qquad \text{and} \qquad b \mid m.$$

So

$$dx \mid m \qquad \text{and} \qquad dy \mid m.$$

Hence

$$x \mid \frac{m}{d} \qquad \text{and} \qquad y \mid \frac{m}{d}.$$

Since

$$\gcd(x, y) = 1,$$

it follows that

$$xy \mid \frac{m}{d}.$$

Thus

$$dxy \mid m.$$

So dxy divides every common multiple of a and b, which means it is the least common multiple. Therefore

$$lcm[a, b] = dxy.$$

But

$$\frac{ab}{\gcd(a, b)} = \frac{(dx)(dy)}{d} = dxy.$$

Hence

$$lcm[a, b] = \frac{ab}{\gcd(a, b)}.$$

□

[12.2.0.6] Problem. Prove that:

(a)

$$\gcd(a, b) \mid \gcd(a + b, a - b).$$

(b) If a is odd and b is even, then

$$\gcd(a, b) = \gcd(a + b, a - b).$$

(c) If a and b are odd, then

$$2 \gcd(a, b) = \gcd(a + b, a - b).$$

∴

Solution. (a). Let

$$d = \gcd(a, b).$$

Then

$$d \mid a \qquad \text{and} \qquad d \mid b.$$

Hence

$$d \mid (a+b) \qquad \text{and} \qquad d \mid (a-b).$$

Therefore d is a common divisor of $a+b$ and $a-b$, so

$$d \mid \gcd(a+b, a-b).$$

(b). Let

$$d = \gcd(a, b).$$

By part (a),

$$d \mid \gcd(a+b, a-b).$$

Now let

$$e = \gcd(a+b, a-b).$$

Then

$$e \mid (a+b) \qquad \text{and} \qquad e \mid (a-b).$$

So

$$e \mid ((a+b)+(a-b)) = 2a$$

and

$$e \mid ((a+b)-(a-b)) = 2b.$$

Since a is odd and b is even, any common divisor of $a+b$ and $a-b$ must be odd. Thus

$$\gcd(e, 2) = 1.$$

Because

$$e \mid 2a$$

and

$$\gcd(e, 2) = 1,$$

it follows that

$$e \mid a.$$

Similarly,

$$e \mid b.$$

Hence

$$e \mid \gcd(a, b) = d.$$

Together with part (a), this gives

$$\gcd(a, b) = \gcd(a+b, a-b).$$

(c). Let

$$d = \gcd(a, b).$$

Since a and b are odd, write

$$a = da_1 \qquad \text{and} \qquad b = db_1,$$

where

$$\gcd(a_1, b_1) = 1.$$

Because a and b are odd, both a_1 and b_1 are odd. Then

$$a + b = d(a_1 + b_1) \qquad \text{and} \qquad a - b = d(a_1 - b_1).$$

So

$$\gcd(a + b, a - b) = d \cdot \gcd(a_1 + b_1, a_1 - b_1).$$

Now $a_1 + b_1$ and $a_1 - b_1$ are both even, so

$$2 \mid \gcd(a_1 + b_1, a_1 - b_1).$$

Also, if an odd integer divides both $a_1 + b_1$ and $a_1 - b_1$, then it divides their sum and difference:

$$(a_1 + b_1) + (a_1 - b_1) = 2a_1,$$
$$(a_1 + b_1) - (a_1 - b_1) = 2b_1.$$

Since the divisor is odd, it must divide both a_1 and b_1. But

$$\gcd(a_1, b_1) = 1,$$

so no odd divisor greater than 1 can occur. Hence

$$\gcd(a_1 + b_1, a_1 - b_1) = 2.$$

Therefore

$$\gcd(a + b, a - b) = 2d = 2 \gcd(a, b).$$

□

[12.2.0.7] PROBLEM. Use the GCD algorithm to show that the GCD of 166 and 39 is 1 and to find integers x and y such that

$$1 = x166 + y39.$$

Show your work.

∴

Solution. Apply the Euclidean algorithm:

$$166 = 4 \cdot 39 + 10,$$
$$39 = 3 \cdot 10 + 9,$$
$$10 = 1 \cdot 9 + 1,$$
$$9 = 9 \cdot 1 + 0.$$

Hence

$$\gcd(166, 39) = 1.$$

Now work backward to find the extended gcd:

$$1 = 10 - 9,$$
$$= 10 - (39 - 3 \cdot 10),$$

$$= 4 \cdot 10 - 39,$$
$$= 4(166 - 4 \cdot 39) - 39,$$
$$= 4 \cdot 166 - 17 \cdot 39.$$

Thus

$$1 = 4 \cdot 166 + (-17) \cdot 39.$$

So

$$x = 4 \qquad \text{and} \qquad y = -17.$$

□

[12.2.0.8] Problem. Let p be an integer other than $0, \pm 1$. Prove that p is prime if and only if for each $a \in \mathbb{Z}$ either $\gcd(a, p) = 1$ or $p \mid a$.

∴

Solution. **($\Longrightarrow$).** Assume that p is prime. Let $a \in \mathbb{Z}$. If $p \mid a$, then we are done. So suppose $p \nmid a$. We must show that

$$\gcd(a, p) = 1.$$

Let

$$d = \gcd(a, p).$$

Then

$$d \mid p.$$

Since p is prime, its only divisors are

$$\pm 1, \pm p.$$

Because $p \nmid a$, we cannot have $d = \pm p$. Thus

$$d = \pm 1.$$

Since the gcd is positive, it follows that

$$\gcd(a, p) = 1.$$

($\Longleftarrow$). Assume that for each $a \in \mathbb{Z}$, either

$$\gcd(a, p) = 1 \quad \text{or} \quad p \mid a.$$

We prove that p is prime. Let $d \in \mathbb{Z}$ with

$$d \mid p.$$

Then there exists $m \in \mathbb{Z}$ such that

$$p = dm.$$

Apply the given property to $a = d$. Either

$$\gcd(d, p) = 1 \quad \text{or} \quad p \mid d.$$

If

$$\gcd(d, p) = 1,$$

then since $d \mid p$, the only positive possibility is

$$d = 1.$$

If

$$p \mid d,$$

then there exists $t \in \mathbb{Z}$ such that

$$d = pt.$$

Since also

$$d \mid p,$$

we must have

$$d = \pm p.$$

Thus every divisor of p is one of

$$\pm 1, \pm p.$$

Since $p \neq 0, \pm 1$, it follows that p is prime. □

[12.2.0.9] Problem. Let p be an integer other than $0, \pm 1$ with this property: Whenever b and c are integers such that $p \mid bc$, then $p \mid b$ or $p \mid c$. Prove that p is prime.

∴

Solution. Suppose $d \mid p$. Then there exists $t \in \mathbb{Z}$ such that

$$p = dt.$$

Since

$$p \mid dt,$$

the given property implies that

$$p \mid d \quad \text{or} \quad p \mid t.$$

If

$$p \mid d,$$

then

$$d = \pm p.$$

If

$$p \mid t,$$

then

$$t = \pm p$$

or at least $|t| \geq |p|$, and since

$$p = dt,$$

this forces

$$d = \pm 1.$$

So every divisor of p is one of

$$\pm 1, \pm p.$$

Since $p \neq 0, \pm 1$, it follows that p is prime. □

[12.2.0.10] Problem. If

$$a = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$$

and

$$b = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k},$$

where $p_1, p_2, \dots, p_k$ are distinct positive primes and each $r_i, s_i \geq 0$, then prove that:

(a)

$$\gcd(a,b) = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k},$$

where for each i,

$$n_i = \min\{r_i, s_i\}.$$

(b)

$$lcm[a,b] = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k},$$

where for each i,

$$t_i = \max\{r_i, s_i\}.$$

Solution. (a). Let

$$d := p_1^{n_1} p_2^{n_2} \dots p_k^{n_k},$$

where

$$n_i = \min\{r_i, s_i\}.$$

We show that $d = \gcd(a,b)$.

First, $d \mid a$ and $d \mid b$. Indeed, for each i,

$$n_i \leq r_i \quad \text{and} \quad n_i \leq s_i,$$

so every prime power appearing in d appears in both a and b with exponent at least n_i. Now let q be any common divisor of a and b. Write

$$q = p_1^{v_1} p_2^{v_2} \dots p_k^{v_k},$$

where each $v_i \geq 0$. Since $q \mid a$, we must have

$$v_i \leq r_i$$

for each i. Since $q \mid b$, we must also have

$$v_i \leq s_i$$

for each i. Hence

$$v_i \leq \min\{r_i, s_i\} = n_i$$

for every i. Therefore

$$q \mid d.$$

So d is a common divisor of a and b, and every common divisor divides d. Hence

$$\gcd(a,b) = d = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}.$$

(b). Let

$$t_i = \max\{r_i, s_i\}$$

for each i, and define

$$m := p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}.$$

We show that

$$lcm[a,b] = m.$$

First, $a \mid m$ and $b \mid m$. Indeed, for each i,

$$r_i \le t_i \quad \text{and} \quad s_i \le t_i.$$

So m is a common multiple of a and b.

Now let N be any common multiple of a and b. Write

$$N = p_1^{w_1} p_2^{w_2} \dots p_k^{w_k} \cdot u,$$

where u is not divisible by any of the primes p_i. Since $a \mid N$, we have

$$r_i \le w_i$$

for each i. Since $b \mid N$, we also have

$$s_i \le w_i$$

for each i. Therefore

$$t_i = \max\{r_i, s_i\} \le w_i$$

for every i. So

$$m \mid N.$$

Thus m is a common multiple of a and b, and it divides every common multiple. Hence

$$lcm[a,b] = m = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}.$$

□

[12.2.0.11] Problem. Prove that

$$a \mid b \quad \text{if and only if} \quad a^2 \mid b^2.$$

Solution. **($\Longrightarrow$).** Suppose

$$a \mid b.$$

Then there exists $x \in \mathbb{Z}$ such that

$$b = ax.$$

Squaring both sides gives

$$b^2 = a^2 x^2.$$

Hence

$$a^2 \mid b^2.$$

($\Longleftarrow$). Suppose

$$a^2 \mid b^2.$$

We want to show that

$$a \mid b.$$

Write the prime factorizations of a and b. If

$$a = \pm p_1^{r_1} \cdots p_k^{r_k},$$

then

$$a^2 = p_1^{2r_1} \cdots p_k^{2r_k}.$$

If

$$a^2 \mid b^2,$$

then for each prime p_i, the exponent of p_i in b^2 is at least $2r_i$. So the exponent of p_i in b is at least r_i. Therefore every prime power dividing a also divides b, and hence

$$a \mid b.$$

Thus

$$a \mid b \quad \text{if and only if} \quad a^2 \mid b^2.$$

□

[12.2.0.12] Problem. Let p be prime and $1 < k < p$. Prove that p divides the binomial coefficient

$$\binom{p}{k}.$$

Solution. Recall that

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

Write

$$p! = p(p-1)!.$$

Then

$$\binom{p}{k} = p \cdot \frac{(p-1)!}{k!(p-k)!}.$$

We now show that

$$\frac{(p-1)!}{k!(p-k)!} \in \mathbb{Z}.$$

But this is automatic, since

$$\binom{p}{k}$$

is an integer.

Also, because

$$1 < k < p,$$

both $k!$ and $(p-k)!$ are products of positive integers all strictly less than p. Since p is prime, none of those factors is divisible by p. So the factor of p in the numerator does not cancel.

Therefore

$$p \mid \binom{p}{k}.$$

□

[12.2.0.13] Problem. Let p, q be primes with $p \geq 5$ and $q \geq 5$. Prove that

$$24 \mid (p^2 - q^2).$$

Solution. Since $p, q \geq 5$ are prime, both are odd. Thus

$$p^2 - q^2 = (p-q)(p+q).$$

We first show that

$$8 \mid (p^2 - q^2).$$

Every odd integer is congruent to either 1, 3, 5, or 7 modulo 8, and in each case its square is congruent to 1 modulo 8. So

$$p^2 \equiv 1 \pmod 8 \quad \text{and} \quad q^2 \equiv 1 \pmod 8.$$

Hence

$$p^2 - q^2 \equiv 0 \pmod 8.$$

Therefore

$$8 \mid (p^2 - q^2).$$

Next we show that

$$3 \mid (p^2 - q^2).$$

Since p and q are primes at least 5, neither is divisible by 3. So each is congruent to either 1 or -1 modulo 3. Hence

$$p^2 \equiv 1 \pmod 3 \quad \text{and} \quad q^2 \equiv 1 \pmod 3.$$

Therefore

$$p^2 - q^2 \equiv 0 \pmod 3,$$

so

$$3 \mid (p^2 - q^2).$$

Since

$$\gcd(8,3) = 1,$$

it follows that

$$24 = 8 \cdot 3 \mid (p^2 - q^2).$$

Hence

$$24 \mid (p^2 - q^2).$$

□

[12.2.0.14] Problem. Prove that:

(a)

$$(n-a)^2 \equiv a^2 \mod n.$$

(b)

$$(2n-a)^2 \equiv a^2 \mod 4n.$$

∴

Solution. **(a).** By the definition of congruence, we must show that

$$n \mid a^2 - (n-a)^2.$$

Compute:

$$\begin{aligned} a^2 - (n-a)^2 &= a^2 - (n^2 - 2an + a^2) \\ &= 2an - n^2 \\ &= n(2a-n). \end{aligned}$$

Since the right-hand side is a multiple of n, we conclude that

$$(n-a)^2 \equiv a^2 \mod n.$$

(b). By the definition of congruence, we must show that

$$4n \mid a^2 - (2n-a)^2.$$

Compute:

$$\begin{aligned} a^2 - (2n-a)^2 &= a^2 - (4n^2 - 4an + a^2) \\ &= 4an - 4n^2 \\ &= 4n(a-n). \end{aligned}$$

Since the right-hand side is a multiple of $4n$, we conclude that

$$(2n-a)^2 \equiv a^2 \mod 4n.$$

□

[12.2.0.15] Problem. If $p \geq 5$ and p is prime, prove that $[p] = [1]$ or $[p] = [5]$ in $\mathbb{Z}_6$.

∴

Solution. Theorem 2.3 states that

$$[a] = [b] \quad \text{if and only if} \quad a \equiv b \mod n.$$

Since we are in $\mathbb{Z}_6$, this means

$$[p] = [1] \quad \text{if and only if} \quad p \equiv 1 \mod 6,$$

and

$$[p] = [5] \quad \text{if and only if} \quad p \equiv 5 \mod 6.$$

Also,

$$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}.$$

We prove that $[p]$ cannot be any of $[0], [2], [3], [4]$. Since p is prime and $p \geq 5$, p is odd. Therefore p cannot be congruent to 2 or 4 modulo 6, because those are even classes. Also, p cannot be congruent to 0 modulo 6, since that would mean

$$6 \mid p,$$

which is impossible for a prime $p \geq 5$. If $[p] = [3]$, then

$$p \equiv 3 \mod 6,$$

so

$$p = 6k + 3 = 3(2k + 1)$$

for some $k \in \mathbb{Z}$. Thus $3 \mid p$. Since p is prime and $p \geq 5$, this is impossible. Therefore $[p]$ cannot be $[0], [2], [3]$, or $[4]$ in $\mathbb{Z}_6$. Hence the only remaining possibilities are

$$[p] = [1] \quad \text{or} \quad [p] = [5].$$

□

[12.2.0.16] Problem. Prove that

$$10^n \equiv (-1)^n \mod 11$$

for every positive integer n.

∴

Solution. We prove this using mathematical induction. For the base case, let $n = 1$. Then

$$10^1 \equiv (-1)^1 \mod 11$$
$$10 \equiv -1 \mod 11,$$

which is true since

$$11 \mid (-1) - 10 = -11.$$

Now define

$$S := \{x \in \mathbb{Z}^+ : 10^x \equiv (-1)^x \mod 11\},$$

and we will show that

$$S = \mathbb{Z}^+.$$

Assume $n \in S$. Then

$$10^n \equiv (-1)^n \mod 11.$$

We must show that

$$10^{n+1} \equiv (-1)^{n+1} \mod 11.$$

Now

$$10^{n+1} = 10 \cdot 10^n.$$

Also,

$$(-1)^{n+1} = (-1) \cdot (-1)^n.$$

Since

$$10 \equiv -1 \mod 11$$

and

$$10^n \equiv (-1)^n \mod 11,$$

Theorem 2.2 implies that

$$10 \cdot 10^n \equiv (-1) \cdot (-1)^n \mod 11.$$

So

$$10^{n+1} \equiv (-1)^{n+1} \mod 11.$$

Thus

$$n+1 \in S.$$

Therefore, by the Principle of Mathematical Induction,

$$S = \mathbb{Z}^+.$$

Hence

$$10^n \equiv (-1)^n \mod 11$$

for every positive integer n. □

[12.2.0.17] Problem. (a) Prove or disprove: If

$$a^2 \equiv b^2 \mod n,$$

then

$$a \equiv b \mod n \quad \text{or} \quad a \equiv -b \mod n.$$

(b) Do part (a) when n is prime.

∴

Solution. (a). This statement is false in general. A disproof by example is given by

$$a = 6, \qquad b = 1, \qquad n = 35.$$

Then

$$6^2 = 36 \equiv 1 = 1^2 \mod 35.$$

So

$$a^2 \equiv b^2 \mod 35.$$

However,

$$6 \not\equiv 1 \mod 35$$

and

$$6 \not\equiv -1 \mod 35.$$

Thus the statement is false.

[12.2.0.18] Remark. I have found some commonality for part (a). I noticed that the product of twin primes can equal n, and a and b are some sum and difference between the two, generally a being one less than the higher twin and $b = 1$. From what I have calculated, this seems to be the general idea, but I have not proven it for all twin primes. So it is still a conjecture.

$$a = 4,\ b = 1,\ n = 15$$
$$a = 12,\ b = 1,\ n = 143$$
$$a = 18,\ b = 1,\ n = 323$$

And so forth.

(b). Now assume that n is prime. Since

$$a^2 \equiv b^2 \mod n,$$

we have

$$n \mid b^2 - a^2.$$

Factor:

$$b^2 - a^2 = (b - a)(b + a).$$

So

$$n \mid (b - a)(b + a).$$

Since n is prime, Euclid's Lemma implies that

$$n \mid (b - a) \quad \text{or} \quad n \mid (b + a).$$

If

$$n \mid (b - a),$$

then

$$a \equiv b \mod n.$$

If

$$n \mid (b + a),$$

then

$$a \equiv -b \mod n.$$

Thus, when n is prime,

$$a^2 \equiv b^2 \mod n \implies a \equiv b \mod n \quad \text{or} \quad a \equiv -b \mod n.$$

□

[12.2.0.19] Problem. As we have clearly stated in class, and given the defined answer for parts (a) and (b), prove the following.

(a) If a is a unit in $\mathbb{Z}_n$, prove that a is not a zero divisor.

(b) If a is a zero divisor in $\mathbb{Z}_n$, prove that a is not a unit.

$\therefore$

Solution. **(a).** Assume, by the definition of a unit, that

$$\gcd(a, n) = 1.$$

Suppose there is a $b \in \mathbb{Z}$ with

$$[a][b] = [0].$$

To show that $[a]$ is not a zero divisor, we must prove that this implies

$$[b] = [0].$$

By the previous theorem, $[a]$ is a unit in $\mathbb{Z}_n$, so there exists $x \in \mathbb{Z}$ such that

$$[x][a] = [1].$$

Then

$$\begin{aligned}[x]([a][b]) &= [x][0] \\ &= [x \cdot 0] \\ &= [0].\end{aligned}$$

By associativity,

$$\begin{aligned}([x][a])[b] &= [0] \\ [1][b] &= [0] \\ [b] &= [0].\end{aligned}$$

Hence $[a]$ is not a zero divisor.

(b). Conversely, suppose that

$$\gcd(a, n) = d > 1.$$

Then

$$d \mid a \qquad \text{and} \qquad d \mid n.$$

So

$$a = d\left(\frac{a}{d}\right) \qquad \text{and} \qquad n = d\left(\frac{n}{d}\right),$$

where

$$\frac{a}{d}, \frac{n}{d} \in \mathbb{Z}.$$

Now

$$[a]\left[\frac{n}{d}\right] = \left[a \cdot \frac{n}{d}\right] = \left[d \cdot \frac{a}{d} \cdot \frac{n}{d}\right] = \left[n \cdot \frac{a}{d}\right] = [0].$$

Since $d > 1$, we have

$$\left[\frac{n}{d}\right] \neq [0]$$

in $\mathbb{Z}_n$. Thus $[a]$ is a zero divisor. Therefore, if a is a zero divisor in $\mathbb{Z}_n$, then a is not a unit. $\square$

[12.2.0.20] Problem. Prove that every nonzero element of $\mathbb{Z}_n$ is either a unit or a zero divisor, but not both.

$\therefore$

Solution. Let $[a] \neq [0]$ in $\mathbb{Z}_n$. If

$$\gcd(a, n) = 1,$$

then by the previous theorem $[a]$ is a unit. If

$$\gcd(a, n) \neq 1,$$

then since $[a] \neq [0]$, we have

$$\gcd(a, n) = d > 1,$$

and by the previous problem $[a]$ is a zero divisor. So every nonzero element of $\mathbb{Z}_n$ is either a unit or a zero divisor. Now we show it cannot be both. Suppose $[a]$ is both a unit and a zero divisor. Then there exist $[b], [c] \in \mathbb{Z}_n$ with

$$[b] \neq [0], \qquad [a][b] = [0], \qquad [a][c] = [1].$$

Then

$$([a][b])[c] = [0][c] = [0].$$

By associativity,

$$([a][c])[b] = [1][b] = [b].$$

But the left-hand sides are equal by associativity and commutativity of multiplication in $\mathbb{Z}_n$, so we get

$$[b] = [0],$$

a contradiction. Therefore every nonzero element of $\mathbb{Z}_n$ is either a unit or a zero divisor, but not both. □

[12.2.0.21] Problem. Find the multiplicative inverse of $[9]$ in $\mathbb{Z}_{41}$.

$\therefore$

Solution. We want to find $[x]$ such that

$$[9][x] = [1].$$

This is the same as finding integers x and q such that

$$9x = 1 + 41q,$$

or equivalently,

$$9x - 41q = 1.$$

Since

$$\gcd(41, 9) = 1,$$

there exist integers x and y such that

$$9x + 41y = 1.$$

We find them using the Euclidean algorithm:

$$\begin{aligned} 41 &= 4\cdot 9 + 5, \\ 9 &= 1\cdot 5 + 4, \\ 5 &= 1\cdot 4 + 1, \\ 4 &= 4\cdot 1 + 0. \end{aligned}$$

Now work backward:

$$\begin{aligned} 1 &= 5 - 1\cdot 4 \\ &= 5 - (9 - 1\cdot 5) \\ &= 2\cdot 5 - 9 \\ &= 2(41 - 4\cdot 9) - 9 \\ &= 2\cdot 41 - 9\cdot 9. \end{aligned}$$

So

$$(-9)9 + 2\cdot 41 = 1.$$

Thus

$$[-9][9] = [1]$$

in $\mathbb{Z}_{41}$. Since

$$-9 \equiv 32 \mod 41,$$

the multiplicative inverse of $[9]$ in $\mathbb{Z}_{41}$ is

$$[32].$$

□

12.3 Chapter 4

[12.3.0.1] Problem. Let d be an integer that is not a perfect square. Show that

$$\mathbb{Q}\left(\sqrt{d}\right) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$$

is a subfield of $\mathbb{C}$.

∴

Solution. A field is a commutative ring with identity in which every nonzero element has a multiplicative inverse. Thus we must show that this set is closed under addition, additive inverses, multiplication, and multiplicative inverses for nonzero elements. Let

$$q = a_1 + b_1\sqrt{d} \qquad \text{and} \qquad p = a_2 + b_2\sqrt{d}.$$

Then

$$q - p = (a_1 + b_1\sqrt{d}) - (a_2 + b_2\sqrt{d})$$

$$= (a_1 - a_2) + (b_1 - b_2)\sqrt{d}.$$

Since $a_1 - a_2 \in \mathbb{Q}$ and $b_1 - b_2 \in \mathbb{Q}$, this shows closure under subtraction, and hence also under addition and additive inverses. Now check multiplication:

$$\begin{aligned} qp &= (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) \\ &= a_1a_2 + a_1b_2\sqrt{d} + a_2b_1\sqrt{d} + b_1b_2d \\ &= (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d}. \end{aligned}$$

Since $d \in \mathbb{Z} \subseteq \mathbb{Q}$, the coefficients are rational. Thus $\mathbb{Q}\left(\sqrt{d}\right)$ is closed under multiplication. Also,

$$0 = 0 + 0\sqrt{d} \in \mathbb{Q}\left(\sqrt{d}\right)$$

and

$$1 = 1 + 0\sqrt{d} \in \mathbb{Q}\left(\sqrt{d}\right).$$

Now let

$$w = a + b\sqrt{d} \in \mathbb{Q}\left(\sqrt{d}\right), \qquad w \neq 0.$$

We must show that $w^{-1} \in \mathbb{Q}\left(\sqrt{d}\right)$. Compute:

$$\begin{aligned} \frac{1}{a + b\sqrt{d}} &= \frac{1}{a + b\sqrt{d}} \cdot \frac{a - b\sqrt{d}}{a - b\sqrt{d}} \\ &= \frac{a - b\sqrt{d}}{a^2 - b^2d} \\ &= \frac{a}{a^2 - b^2d} + \frac{-b}{a^2 - b^2d}\sqrt{d}. \end{aligned}$$

So it remains to show that

$$a^2 - b^2d \neq 0.$$

If

$$a^2 - b^2d = 0,$$

then

$$a^2 = b^2d.$$

If $b = 0$, then $a = 0$, which would give $w = 0$, a contradiction. So $b \neq 0$. Then

$$d = \left(\frac{a}{b}\right)^2.$$

This would mean d is a square in $\mathbb{Q}$. Since $d \in \mathbb{Z}$, that would imply d is a perfect square in $\mathbb{Z}$, contradicting the hypothesis. Thus

$$a^2 - b^2d \neq 0,$$

and so $w^{-1} \in \mathbb{Q}\left(\sqrt{d}\right)$. Therefore $\mathbb{Q}\left(\sqrt{d}\right)$ is a subfield of $\mathbb{C}$. □

[12.3.0.2] Problem. If u is a unit in a commutative ring R with identity, prove that u is not a zero divisor.

———— ∴ ————

Solution. Suppose u is a unit. Then there exists $u^{-1} \in R$ such that

$$uu^{-1} = 1.$$

Now suppose, for contradiction, that u is also a zero divisor. Then there exists $x \in R$, $x \neq 0$, such that

$$ux = 0.$$

Multiply both sides by u^{-1}:

$$\begin{aligned} u^{-1}(ux) &= u^{-1}0 \\ (u^{-1}u)x &= 0 \\ 1x &= 0 \\ x &= 0. \end{aligned}$$

This contradicts the fact that $x \neq 0$. Therefore u is not a zero divisor. □

[12.3.0.3] Problem. Which of the following functions are homomorphisms?

(a)

$$f : \mathbb{Z} \mapsto \mathbb{Z}, \qquad f(x) = -x.$$

(e)

$$f : \mathbb{Z}_{12} \mapsto \mathbb{Z}_4$$

defined by

$$f([x]_{12}) = [x]_4.$$

Solution. **(a).** We check whether this function preserves addition and multiplication. For addition,

$$f(a+b) = -(a+b) = -a - b = f(a) + f(b).$$

So it preserves addition. For multiplication,

$$f(ab) = -(ab),$$

but

$$f(a)f(b) = (-a)(-b) = ab.$$

In general,

$$-(ab) \neq ab,$$

so f does not preserve multiplication. Therefore this function is not a ring homomorphism.

(e). We first show that the function is well-defined. Suppose

$$[x]_{12} = [y]_{12}.$$

Then

$$x \equiv y \mod 12,$$

so

$$12 \mid (x - y).$$

Hence

$$4 \mid (x - y),$$

which means

$$x \equiv y \mod 4.$$

Thus

$$[x]_4 = [y]_4.$$

So the map is well-defined. Now check addition:

$$\begin{aligned} f([x]_{12} + [y]_{12}) &= f([x + y]_{12}) \\ &= [x + y]_4 \\ &= [x]_4 + [y]_4 \\ &= f([x]_{12}) + f([y]_{12}). \end{aligned}$$

Now check multiplication:

$$\begin{aligned} f([x]_{12}[y]_{12}) &= f([xy]_{12}) \\ &= [xy]_4 \\ &= [x]_4[y]_4 \\ &= f([x]_{12})f([y]_{12}). \end{aligned}$$

Therefore this function is a homomorphism. □

[12.3.0.4] Problem. Let R and S be rings.

(a) Prove that

$$f : R \times S \mapsto R$$

given by

$$f((r, s)) = r$$

is a surjective homomorphism.

(b) Prove that

$$g : R \times S \mapsto S$$

given by

$$g((r, s)) = s$$

is a surjective homomorphism.

(c) If both R and S are nonzero rings, prove that the homomorphisms f and g are not injective.

∴

Solution. (a). First we show surjectivity. Let $r \in R$. Choose any $s \in S$. Then

$$f((r, s)) = r.$$

So f is surjective. Now check addition:

$$\begin{aligned} f((r_1, s_1) + (r_2, s_2)) &= f((r_1 + r_2, s_1 + s_2)) \\ &= r_1 + r_2 \\ &= f((r_1, s_1)) + f((r_2, s_2)). \end{aligned}$$

Now check multiplication:

$$\begin{aligned} f((r_1, s_1)(r_2, s_2)) &= f((r_1 r_2, s_1 s_2)) \\ &= r_1 r_2 \\ &= f((r_1, s_1)) f((r_2, s_2)). \end{aligned}$$

Thus f is a surjective homomorphism.

(b). First we show surjectivity. Let $s \in S$. Choose any $r \in R$. Then

$$g((r, s)) = s.$$

So g is surjective. Now check addition:

$$\begin{aligned} g((r_1, s_1) + (r_2, s_2)) &= g((r_1 + r_2, s_1 + s_2)) \\ &= s_1 + s_2 \\ &= g((r_1, s_1)) + g((r_2, s_2)). \end{aligned}$$

Now check multiplication:

$$\begin{aligned} g((r_1, s_1)(r_2, s_2)) &= g((r_1 r_2, s_1 s_2)) \\ &= s_1 s_2 \\ &= g((r_1, s_1)) g((r_2, s_2)). \end{aligned}$$

Thus g is a surjective homomorphism.

(c). Since both R and S are nonzero rings, choose

$$s_1, s_2 \in S \qquad \text{with} \qquad s_1 \neq s_2,$$

and choose any $r \in R$. Then

$$f((r, s_1)) = r = f((r, s_2)),$$

but

$$(r, s_1) \neq (r, s_2).$$

So f is not injective. Similarly, choose

$$r_1, r_2 \in R \qquad \text{with} \qquad r_1 \neq r_2,$$

and choose any $s \in S$. Then

$$g((r_1, s)) = s = g((r_2, s)),$$

but

$$(r_1, s) \neq (r_2, s).$$

So g is not injective. □

[12.3.0.5] Problem. Show that the first ring is not isomorphic to the second.

(e)

$$\mathbb{Z} \times \mathbb{Z}_2 \qquad \text{and} \qquad \mathbb{Z}.$$

(f)

$$\mathbb{Z}_4 \times \mathbb{Z}_4 \qquad \text{and} \qquad \mathbb{Z}_{16}.$$

$\therefore$

Solution. **(e).** In

$$\mathbb{Z} \times \mathbb{Z}_2,$$

the element

$$(0, [1])$$

is a nontrivial idempotent, since

$$(0, [1])^2 = (0, [1]).$$

But in $\mathbb{Z}$, the only idempotent elements are 0 and 1, because if

$$x^2 = x,$$

then

$$x(x-1) = 0,$$

so

$$x = 0 \quad \text{or} \quad x = 1.$$

A ring isomorphism preserves idempotents. Since $\mathbb{Z} \times \mathbb{Z}_2$ has a nontrivial idempotent different from $(0, [0])$ and $(1, [1])$, while $\mathbb{Z}$ does not, the rings are not isomorphic.

(f). In

$$\mathbb{Z}_4 \times \mathbb{Z}_4,$$

the element

$$([2], [0])$$

has additive order 2, since

$$([2], [0]) + ([2], [0]) = ([0], [0]).$$

So this ring has nonzero elements of additive order 2. In $\mathbb{Z}_{16}$, the additive group is cyclic of order 16, and it has exactly one element of additive order 2, namely $[8]$. In contrast, $\mathbb{Z}_4 \times \mathbb{Z}_4$ has three nonzero elements of additive order 2:

$$([2], [0]), \quad ([0], [2]), \quad ([2], [2]).$$

An isomorphism of rings induces an isomorphism of additive groups, so it must preserve the number of elements of each order. Therefore

$$\mathbb{Z}_4 \times \mathbb{Z}_4 \ncong \mathbb{Z}_{16}.$$

□

[12.3.0.6] Problem. Let F be a field and

$$f : F \mapsto R$$

a homomorphism of rings.

(a) If there is a nonzero element c of F such that

$$f(c) = 0_R,$$

prove that f is the zero homomorphism.

(b) Prove that f is either injective or the zero homomorphism.

$\therefore$

Solution. (a). Assume there is a nonzero element $c \in F$ such that

$$f(c) = 0_R.$$

Since F is a field and $c \neq 0$, c is a unit. So there exists $c^{-1} \in F$ such that

$$cc^{-1} = 1.$$

Now let $x \in F$. Then

$$\begin{aligned} f(x) &= f(x \cdot 1) \\ &= f(xcc^{-1}) \\ &= f(x)f(c)f(c^{-1}) \\ &= f(x) \cdot 0_R \cdot f(c^{-1}) \\ &= 0_R. \end{aligned}$$

Since this is true for every $x \in F$, f is the zero homomorphism.

(b). We prove the contrapositive. Suppose f is not injective. Then there exist $a, b \in F$ with $a \neq b$ such that

$$f(a) = f(b).$$

Thus

$$f(a - b) = 0_R.$$

Since $a \neq b$, we have

$$a - b \neq 0.$$

By part (a), it follows that f is the zero homomorphism. Therefore, if f is not the zero homomorphism, then f must be injective. So f is either injective or the zero homomorphism. □

[12.3.0.7] Problem. Let $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$, and let

$$f : \mathbb{Z}_{mn} \mapsto \mathbb{Z}_m \times \mathbb{Z}_n$$

be the function given by

$$f([a]_{mn}) = ([a]_m, [a]_n).$$

(a) Show that the map f is well-defined.

(b) Prove that f is an isomorphism.

Solution. (a). Suppose

$$[a]_{mn} = [b]_{mn}$$

in $\mathbb{Z}_{mn}$. Then

$$a \equiv b \mod mn,$$

so

$$mn \mid (a-b).$$

Hence

$$m \mid (a-b) \qquad \text{and} \qquad n \mid (a-b).$$

Therefore

$$[a]_m = [b]_m \qquad \text{and} \qquad [a]_n = [b]_n.$$

So

$$f([a]_{mn}) = ([a]_m, [a]_n) = ([b]_m, [b]_n) = f([b]_{mn}).$$

Thus f is well-defined.

(b). First we show that f is a homomorphism. For addition,

$$\begin{aligned} f([a]_{mn} + [b]_{mn}) &= f([a+b]_{mn}) \\ &= ([a+b]_m, [a+b]_n) \\ &= ([a]_m, [a]_n) + ([b]_m, [b]_n) \\ &= f([a]_{mn}) + f([b]_{mn}). \end{aligned}$$

For multiplication,

$$\begin{aligned} f([a]_{mn}[b]_{mn}) &= f([ab]_{mn}) \\ &= ([ab]_m, [ab]_n) \\ &= ([a]_m, [a]_n)([b]_m, [b]_n) \\ &= f([a]_{mn}) f([b]_{mn}). \end{aligned}$$

Now show injectivity. Suppose

$$f([a]_{mn}) = f([b]_{mn}).$$

Then

$$([a]_m, [a]_n) = ([b]_m, [b]_n),$$

so

$$[a]_m = [b]_m \qquad \text{and} \qquad [a]_n = [b]_n.$$

Thus

$$m \mid (a-b) \qquad \text{and} \qquad n \mid (a-b).$$

Since

$$\gcd(m, n) = 1,$$

it follows that

$$mn \mid (a-b).$$

Therefore

$$[a]_{mn} = [b]_{mn}.$$

So f is injective. Now show surjectivity. Let

$$([r]_m, [s]_n) \in \mathbb{Z}_m \times \mathbb{Z}_n.$$

Since

$$\gcd(m,n) = 1,$$

there exist $u, v \in \mathbb{Z}$ such that

$$um + vn = 1.$$

Set

$$c = svn + rum.$$

Then modulo m, we have

$$svn \equiv s(1-um) \equiv s \mod m$$

and

$$rum \equiv 0 \mod m.$$

So

$$c \equiv s \mod m$$

is not quite what we want. Instead use the standard choice

$$c = r(vn) + s(um).$$

Then modulo m,

$$vn \equiv 1 \mod m \qquad \text{and} \qquad um \equiv 0 \mod m,$$

so

$$c \equiv r \mod m.$$

Similarly, modulo n,

$$um \equiv 1 \mod n \qquad \text{and} \qquad vn \equiv 0 \mod n,$$

so

$$c \equiv s \mod n.$$

Hence

$$f([c]_{mn}) = ([r]_m, [s]_n).$$

So f is surjective. Therefore f is a bijective homomorphism, hence an isomorphism. □

[12.3.0.8] Problem. If $\gcd(m,n) \neq 1$, prove that $\mathbb{Z}_{mn}$ is not isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$.

∴

Solution. Let

$$d = \gcd(m,n) > 1.$$

Then we can write

$$m = dq \qquad \text{and} \qquad n = ds$$

for some integers q, s. Consider the element

$$[mq]_{mn} = [m]_{mn} \cdot [q]_{mn},$$

but an easier choice is

$$[dqs]_{mn}.$$

Since

$$mn = d^2 qs,$$

we have

$$dqs \not\equiv 0 \mod mn$$

in general, but under the map

$$[a]_{mn} \mapsto ([a]_m, [a]_n),$$

we get

$$[dqs]_m = [0]_m$$

because

$$dqs = \frac{mn}{d}$$

is a multiple of $m = dq$. Similarly,

$$[dqs]_n = [0]_n$$

because it is also a multiple of $n = ds$. So the natural map sends a nonzero class in $\mathbb{Z}_{mn}$ to

$$([0]_m, [0]_n).$$

Thus the natural map is not injective. Now if

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n,$$

then their additive groups would also be isomorphic. But in $\mathbb{Z}_{mn}$, the additive group is cyclic. On the other hand, when $\gcd(m, n) \neq 1$, the additive group

$$\mathbb{Z}_m \times \mathbb{Z}_n$$

is not cyclic. Therefore the rings cannot be isomorphic. Hence, if

$$\gcd(m, n) \neq 1,$$

then

$$\mathbb{Z}_{mn} \ncong \mathbb{Z}_m \times \mathbb{Z}_n.$$

□

12.4 Chapter 5

[12.4.0.1] Problem. Which of the following subsets of $R[x]$ are subrings of $R[x]$? Justify your answer.

(a) All polynomials with constant term 0_R.

(b) All polynomials of degree 2.

(c) All polynomials of degree $\leq k$, where k is a fixed positive integer.

(d) All polynomials in which the odd powers of x have zero coefficients.

(e) All polynomials in which the even powers of x have zero coefficients.

Solution. **(a).** Let

$$S[x] := \{f(x) \in R[x] : \text{the constant term of } f(x) \text{ is } 0_R\}.$$

We show that $S[x]$ is a subring of $R[x]$. If $y(x), z(x) \in S[x]$, then both have constant term 0_R. Therefore the constant term of $y(x) + z(x)$ is

$$0_R + 0_R = 0_R,$$

so $y(x) + z(x) \in S[x]$. Also, the constant term of $-y(x)$ is

$$-0_R = 0_R,$$

so $-y(x) \in S[x]$. For multiplication, if $y(x), z(x) \in S[x]$, then the constant term of $y(x)z(x)$ is the product of the constant terms:

$$0_R \cdot 0_R = 0_R.$$

So $y(x)z(x) \in S[x]$. Finally, the zero polynomial is in $S[x]$. Thus $S[x]$ is a subring of $R[x]$.

(b). This is not a subring of $R[x]$. A subring must contain the zero polynomial. But the zero polynomial does not have degree 2. Also, the sum of two degree 2 polynomials need not have degree 2. For example, in any ring,

$$x^2 + 1 \quad \text{and} \quad -(x^2 + 1)$$

both have degree 2, but their sum is the zero polynomial. Thus this set is not a subring.

(c). This is not a subring of $R[x]$ in general. It is closed under addition and contains the zero polynomial, but it is not closed under multiplication. If $f(x)$ and $g(x)$ both have degree k, then in general

$$\deg(f(x)g(x)) = 2k,$$

which is greater than k. Therefore this set is not a subring.

(d). Let $S[x] \subseteq R[x]$ be the set of all polynomials in which the odd powers of x have zero coefficients. Then every element of $S[x]$ can be written in the form

$$\sum_{i=0}^{n} a_i x^{2i}.$$

If

$$y(x) = \sum_{i=0}^{n} a_i x^{2i} \qquad \text{and} \qquad z(x) = \sum_{j=0}^{m} b_j x^{2j},$$

then

$$y(x) + z(x)$$

still has only even powers of x. So $S[x]$ is closed under addition. Also,

$$-y(x) = \sum_{i=0}^{n} (-a_i)x^{2i},$$

so $S[x]$ is closed under additive inverses. For multiplication,

$$y(x)z(x) = \left(\sum_{i=0}^{n} a_i x^{2i}\right)\left(\sum_{j=0}^{m} b_j x^{2j}\right).$$

Every term in this product has the form

$$a_i b_j x^{2i+2j} = a_i b_j x^{2(i+j)},$$

which again has even exponent. So $y(x)z(x) \in S[x]$. Also, the zero polynomial lies in $S[x]$. Thus $S[x]$ is a subring of $R[x]$.

(e). This is not a subring. It is not closed under multiplication. For example,

$$x \in S[x],$$

but

$$x \cdot x = x^2,$$

and x^2 has a nonzero even-power coefficient. So $x^2 \notin S[x]$. Also, the zero polynomial issue depends on convention, but the failure of closure under multiplication already shows this is not a subring. □

[12.4.0.2] Problem. Use the Euclidean Algorithm to find the gcd of

$$x^4 + 3x^3 + 2x + 4 \quad \text{and} \quad x^2 - 1$$

in $\mathbb{Z}_5[x]$.

∴

Solution. Using the division algorithm in $\mathbb{Z}_5[x]$, divide

$$x^4 + 3x^3 + 2x + 4$$

by

$$x^2 - 1.$$

First,

$$x^4 + 3x^3 + 2x + 4 = x^2(x^2 - 1) + (3x^3 + x^2 + 2x + 4).$$

Now divide the remainder by $x^2 - 1$ again:

$$\begin{aligned} 3x^3 + x^2 + 2x + 4 &= 3x(x^2 - 1) + (x^2 + 5x + 4) \\ &= 3x(x^2 - 1) + (x^2 + 4). \end{aligned}$$

Then

$$\begin{aligned} x^2 + 4 &= 1 \cdot (x^2 - 1) + 5 \\ &= 1 \cdot (x^2 - 1) + 0. \end{aligned}$$

So altogether,

$$x^4+3x^3+2x+4=(x^2+3x+1)(x^2-1)+0.$$

Hence

$$x^2-1 \mid x^4+3x^3+2x+4.$$

Therefore the gcd is

$$\gcd(x^4+3x^3+2x+4,\ x^2-1)=x^2-1.$$

Since x^2-1 is already monic, this is the gcd. □

[12.4.0.3] Problem. Express the gcd from the previous problem as a linear combination of the two polynomials.

∴

Solution. Since

$$\gcd(x^4+3x^3+2x+4,\ x^2-1)=x^2-1,$$

we can write the gcd immediately as

$$x^2-1=0\cdot(x^4+3x^3+2x+4)+1\cdot(x^2-1).$$

Thus the gcd is a linear combination of the two polynomials. □

[12.4.0.4] Problem. Let $f(x),g(x),h(x)\in F[x]$, with $f(x)$ and $g(x)$ relatively prime. If $f(x)\mid h(x)$ and $g(x)\mid h(x)$, prove that $f(x)g(x)\mid h(x)$.

∴

Solution. Since $f(x)$ and $g(x)$ are relatively prime, we have

$$\gcd(f(x),g(x))=1.$$

Therefore there exist $c(x),d(x)\in F[x]$ such that

$$1=f(x)c(x)+g(x)d(x).$$

Also, since $f(x)\mid h(x)$ and $g(x)\mid h(x)$, there exist $a(x),b(x)\in F[x]$ such that

$$h(x)=f(x)a(x) \qquad \text{and} \qquad h(x)=g(x)b(x).$$

Now multiply the Bézout identity by $h(x)$:

$$h(x)=h(x)f(x)c(x)+h(x)g(x)d(x).$$

Using the divisibility relations,

$$\begin{aligned} h(x) &= g(x)b(x)f(x)c(x)+f(x)a(x)g(x)d(x) \\ &= f(x)g(x)(b(x)c(x)+a(x)d(x)). \end{aligned}$$

Therefore

$$f(x)g(x)\mid h(x).$$

□

[12.4.0.5] Problem. (a) By counting products of the form $(x+a)(x+b)$, show that there are exactly

$$\frac{p^2+p}{2}$$

monic polynomials of degree 2 that are not irreducible in $\mathbb{Z}_p[x]$.

(b) Show that there are exactly

$$\frac{p^2-p}{2}$$

monic irreducible polynomials of degree 2 in $\mathbb{Z}_p[x]$.

$\therefore$

Solution. (a). A monic quadratic in $\mathbb{Z}_p[x]$ has the form

$$x^2+cx+d,$$

where $c,d \in \mathbb{Z}_p$. So there are exactly

$$p^2$$

monic quadratics total. A monic quadratic is reducible if and only if it can be written as

$$(x+a)(x+b)$$

for some $a,b \in \mathbb{Z}_p$. Now count the number of distinct products of this form. Since

$$(x+a)(x+b) = (x+b)(x+a),$$

the ordered pairs (a,b) and (b,a) give the same polynomial. So we count unordered pairs $\{a,b\}$ with $a,b \in \mathbb{Z}_p$. The number of unordered pairs with repetition allowed from a set of size p is

$$\binom{p+1}{2} = \frac{p^2+p}{2}.$$

Hence there are exactly

$$\frac{p^2+p}{2}$$

monic reducible polynomials of degree 2 in $\mathbb{Z}_p[x]$.

(b). Since every monic quadratic is either reducible or irreducible, the number of monic irreducible quadratics is

$$p^2 - \frac{p^2+p}{2} = \frac{2p^2-(p^2+p)}{2} = \frac{p^2-p}{2}.$$

Thus there are exactly

$$\frac{p^2-p}{2}$$

monic irreducible polynomials of degree 2 in $\mathbb{Z}_p[x]$. □

[12.4.0.6] Problem. (a) Show that x^2+2 is irreducible in $\mathbb{Z}_5[x]$.

(b) Factor $x^4 - 4$ as a product of irreducibles in $\mathbb{Z}_5[x]$.

$\therefore$

Solution. **(a).** A quadratic polynomial over a field is reducible if and only if it has a root. So we check whether

$$x^2 + 2$$

has a root in $\mathbb{Z}_5$. The squares in $\mathbb{Z}_5$ are

$$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 4, \quad 4^2 = 1.$$

So the only square classes are $0, 1, 4$. But

$$x^2 + 2 = 0 \iff x^2 = -2 \equiv 3 \mod 5.$$

Since 3 is not a square in $\mathbb{Z}_5$, the polynomial has no root. Therefore

$$x^2 + 2$$

is irreducible in $\mathbb{Z}_5[x]$.

(b). In $\mathbb{Z}_5[x]$, we have

$$-4 \equiv 1,$$

so

$$x^4 - 4 = x^4 + 1.$$

Now factor:

$$x^4 + 1 = (x^2 + 2)(x^2 - 2),$$

since in $\mathbb{Z}_5$,

$$(x^2 + 2)(x^2 - 2) = x^4 - 4 = x^4 + 1.$$

Now

$$x^2 + 2$$

is irreducible by part (a). Also,

$$x^2 - 2 = x^2 + 3.$$

To see whether this is reducible, check whether 2 is a square mod 5. It is not, since the square classes are $0, 1, 4$. So $x^2 - 2$ has no root in $\mathbb{Z}_5$, and hence is irreducible. Therefore

$$x^4 - 4 = (x^2 + 2)(x^2 - 2)$$

is the factorization into irreducibles in $\mathbb{Z}_5[x]$. □

[12.4.0.7] Problem. Let $\varphi : \mathbb{C} \mapsto \mathbb{C}$ be an isomorphism of rings such that $\varphi(a) = a$ for each $a \in \mathbb{Q}$. Suppose $r \in \mathbb{C}$ is a root of $f(x) \in \mathbb{Q}[x]$. Prove that $\varphi(r)$ is also a root of $f(x)$.

$\therefore$

Solution. Since r is a root of $f(x)$, we have

$$f(r) = 0.$$

Write

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

where each $a_i \in \mathbb{Q}$. Now evaluate f at $\varphi(r)$:

$$f(\varphi(r)) = a_n(\varphi(r))^n + a_{n-1}(\varphi(r))^{n-1} + \cdots + a_1\varphi(r) + a_0.$$

Since φ is a ring isomorphism and fixes every rational number, we have

$$\varphi(a_i) = a_i$$

for all i, and also

$$\varphi(r^k) = \varphi(r)^k.$$

Thus

$$\begin{aligned} f(\varphi(r)) &= \varphi(a_n)\varphi(r^n) + \varphi(a_{n-1})\varphi(r^{n-1}) + \cdots + \varphi(a_1)\varphi(r) + \varphi(a_0) \\ &= \varphi(a_n r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0) \\ &= \varphi(f(r)) \\ &= \varphi(0) \\ &= 0. \end{aligned}$$

Therefore $\varphi(r)$ is also a root of $f(x)$. □

[12.4.0.8] Problem. We say that $a \in F$ is a multiple root of $f(x) \in F[x]$ if $(x-a)^k$ is a factor of $f(x)$ for some $k \geq 2$.

(a) Prove that $a \in \mathbb{R}$ is a multiple root of $f(x) \in \mathbb{R}[x]$ if and only if a is a root of both $f(x)$ and $f'(x)$.

(b) If $f(x) \in \mathbb{R}[x]$ and if $f(x)$ is relatively prime to $f'(x)$, prove that $f(x)$ has no multiple root in $\mathbb{R}[x]$.

∴

Solution. (a). Suppose first that a is a multiple root of $f(x)$. Then

$$f(x) = (x-a)^k g(x)$$

for some $k \geq 2$ and some $g(x) \in \mathbb{R}[x]$. In particular, $(x-a)^2$ divides $f(x)$, so we may write

$$f(x) = (x-a)^2 g(x).$$

Then clearly

$$f(a) = 0.$$

Differentiate:

$$\begin{aligned} f'(x) &= 2(x-a)g(x) + (x-a)^2 g'(x) \\ &= (x-a)(2g(x) + (x-a)g'(x)). \end{aligned}$$

Thus $(x-a) \mid f'(x)$, so

$$f'(a) = 0.$$

Conversely, suppose a is a root of both $f(x)$ and $f'(x)$. Since $f(a) = 0$, we can write

$$f(x) = (x-a)h(x)$$

for some $h(x) \in \mathbb{R}[x]$. Differentiate:

$$f'(x) = h(x) + (x-a)h'(x).$$

Now evaluate at $x = a$:

$$f'(a) = h(a).$$

But $f'(a) = 0$, so

$$h(a) = 0.$$

Hence $(x-a) \mid h(x)$, so

$$h(x) = (x-a)\,j(x)$$

for some $j(x) \in \mathbb{R}[x]$. Therefore

$$f(x) = (x-a)^2\,j(x),$$

so a is a multiple root of $f(x)$.

(b). If $f(x)$ had a multiple root $a \in \mathbb{R}$, then by part (a), a would be a root of both $f(x)$ and $f'(x)$. That would mean $(x-a)$ is a common factor of $f(x)$ and $f'(x)$. But this contradicts the assumption that $f(x)$ and $f'(x)$ are relatively prime. Therefore $f(x)$ has no multiple root in $\mathbb{R}[x]$. □

[12.4.0.9] Problem. Factor $x^{12}-1$ over each of $\mathbb{R}[x]$ and $\mathbb{Q}[x]$.

∴

Solution. We first factor over $\mathbb{Q}[x]$:

$$\begin{aligned} x^{12}-1 &= (x^6-1)(x^6+1) \\ &= (x^3-1)(x^3+1)(x^6+1) \\ &= (x-1)(x^2+x+1)(x+1)(x^2-x+1)(x^6+1). \end{aligned}$$

Now factor

$$x^6+1 = (x^2+1)(x^4-x^2+1).$$

So over $\mathbb{Q}[x]$ we get

$$x^{12}-1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^2+1)(x^4-x^2+1).$$

Now factor further over $\mathbb{R}[x]$. The quartic

$$x^4-x^2+1$$

factors as

$$x^4-x^2+1 = \left(x^2+\sqrt{3}x+1\right)\left(x^2-\sqrt{3}x+1\right).$$

Thus over $\mathbb{R}[x]$,

$$x^{12}-1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^2+1)\left(x^2+\sqrt{3}x+1\right)\left(x^2-\sqrt{3}x+1\right).$$

Therefore,

$$\mathbb{Q}[x] \ni x^{12}-1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^2+1)(x^4-x^2+1),$$

$$\mathbb{R}[x] \ni x^{12}-1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^2+1)(x^2+\sqrt{3}x+1)(x^2-\sqrt{3}x+1).$$

□

[12.4.0.10] Problem. Prove that

$$f(x) = x^4 + x^3 + x^2 + x + 1$$

is irreducible in $\mathbb{Q}[x]$.

$\therefore$

Solution. We use Eisenstein's criterion after shifting by $x \mapsto x+1$. First note that

$$(x-1)f(x) = x^5 - 1,$$

so

$$f(x) = \frac{x^5 - 1}{x - 1}.$$

Then

$$\begin{aligned} f(x+1) &= \frac{(x+1)^5 - 1}{(x+1) - 1} \\ &= \frac{(x+1)^5 - 1}{x}. \end{aligned}$$

Expand:

$$\begin{aligned} (x+1)^5 - 1 &= x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1 - 1 \\ &= x^5 + 5x^4 + 10x^3 + 10x^2 + 5x. \end{aligned}$$

So

$$f(x+1) = x^4 + 5x^3 + 10x^2 + 10x + 5.$$

Now apply Eisenstein's criterion with $p = 5$. We have

$$5 \mid 5,\ 10,\ 10,\ 5,$$

so 5 divides every coefficient except the leading coefficient. Also,

$$5 \nmid 1,$$

and

$$25 \nmid 5.$$

Therefore $f(x+1)$ is irreducible in $\mathbb{Q}[x]$. A polynomial is irreducible if and only if its translate by $x \mapsto x+1$ is irreducible. Hence $f(x)$ is irreducible in $\mathbb{Q}[x]$. □

[12.4.0.11] Problem. Prove that for p prime,

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$$

is irreducible in $\mathbb{Q}[x]$.

$\therefore$

Solution. We use Eisenstein's criterion after the substitution $x \mapsto x+1$. First note that

$$(x-1)f(x) = x^p - 1,$$

so

$$f(x) = \frac{x^p - 1}{x - 1}.$$

Then

$$f(x+1) = \frac{(x+1)^p - 1}{x}.$$

Using the binomial theorem,

$$\begin{aligned}(x+1)^p - 1 &= \sum_{n=0}^{p} \binom{p}{n} x^n - 1 \\ &= \sum_{n=1}^{p} \binom{p}{n} x^n.\end{aligned}$$

So

$$\begin{aligned}f(x+1) &= \frac{\binom{p}{1}x + \binom{p}{2}x^2 + \cdots + \binom{p}{p-1}x^{p-1} + \binom{p}{p}x^p}{x} \\ &= \binom{p}{1} + \binom{p}{2}x + \cdots + \binom{p}{p-1}x^{p-2} + \binom{p}{p}x^{p-1}.\end{aligned}$$

Now for $1 \leq k \leq p-1$, we know that

$$p \mid \binom{p}{k}.$$

Also,

$$\binom{p}{p} = 1,$$

so p does not divide the leading coefficient. Finally,

$$\binom{p}{1} = p,$$

and

$$p^2 \nmid p.$$

Thus Eisenstein's criterion applies with the prime p. Therefore $f(x+1)$ is irreducible in $\mathbb{Q}[x]$. Hence $f(x)$ is irreducible in $\mathbb{Q}[x]$. □

12.5 Chapter 6

[12.5.0.1] Problem. Let $\mathbb{F}$ be a field and $f(x), g(x), p(x) \in \mathbb{F}[x]$ with $p(x)$ nonzero. Then $f(x)$ is congruent to $g(x)$ modulo $p(x)$, written

$$f(x) \equiv g(x) \mod p(x),$$

provided that $p(x)$ divides $f(x) - g(x)$. Prove or disprove: If $p(x)$ is relatively prime to $k(x)$ and

$$f(x)k(x) \equiv g(x)k(x) \mod p(x),$$

then

$$f(x) \equiv g(x) \mod p(x).$$

Solution. This statement is true. Suppose

$$\gcd(p(x), k(x)) = 1_{\mathbb{F}}$$

and

$$f(x)k(x) \equiv g(x)k(x) \mod p(x).$$

By the definition of polynomial congruence modulo $p(x)$, this means

$$p(x) \mid f(x)k(x) - g(x)k(x).$$

Thus

$$p(x) \mid k(x)(f(x) - g(x)).$$

Since $p(x)$ is relatively prime to $k(x)$, Euclid's Lemma for polynomials implies that

$$p(x) \mid f(x) - g(x).$$

Therefore

$$f(x) \equiv g(x) \mod p(x).$$

So the statement is proved. □

[12.5.0.2] Problem. Let $\mathbb{F}$ be a field and $f(x), g(x), p(x) \in \mathbb{F}[x]$ with $p(x)$ nonzero. Then $f(x)$ is congruent to $g(x)$ modulo $p(x)$, written

$$f(x) \equiv g(x) \mod p(x),$$

provided that $p(x)$ divides $f(x) - g(x)$. Prove or disprove: If $p(x)$ is irreducible in $\mathbb{F}[x]$ and

$$f(x)g(x) \equiv 0 \mod p(x),$$

then

$$f(x) \equiv 0 \mod p(x) \quad \text{or} \quad g(x) \equiv 0 \mod p(x).$$

Solution. This statement is true. Suppose $p(x)$ is irreducible in $\mathbb{F}[x]$ and

$$f(x)g(x) \equiv 0 \mod p(x).$$

By the definition of polynomial congruence modulo $p(x)$, this means

$$p(x) \mid f(x)g(x).$$

Since $p(x)$ is irreducible, Euclid's Lemma for polynomials implies that

$$p(x) \mid f(x) \quad \text{or} \quad p(x) \mid g(x).$$

This is equivalent to

$$p(x) \mid f(x) - 0 \quad \text{or} \quad p(x) \mid g(x) - 0.$$

Hence

$$f(x) \equiv 0 \mod p(x) \quad \text{or} \quad g(x) \equiv 0 \mod p(x).$$

□

[12.5.0.3] Problem. Write out the addition and multiplication tables for the congruence class ring

$$\mathbb{Z}_3[x]/(x^2+1).$$

Is $\mathbb{Z}_3[x]/(x^2+1)$ a field?

∴

Solution.

$$x^2 \equiv -1 \equiv 2 \mod (x^2+1),$$

so every congruence class has a representative of the form

$$a+bx$$

with $a, b \in \mathbb{Z}_3$. Thus the elements are

$$0,\ 1,\ 2,\ x,\ x+1,\ x+2,\ 2x,\ 2x+1,\ 2x+2.$$

+	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

·	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Yes, $\mathbb{Z}_3[x]/(x^2+1)$ is a field. The reason is that x^2+1 is irreducible in $\mathbb{Z}_3[x]$. Indeed, the only elements of $\mathbb{Z}_3$ are $0, 1, 2$, and

$$0^2+1=1, \qquad 1^2+1=2, \qquad 2^2+1=4+1\equiv 2 \mod 3,$$

so x^2+1 has no root in $\mathbb{Z}_3$. Hence it is irreducible, and the quotient is a field. □

[12.5.0.4] Problem. Let F be a field. A nonconstant polynomial $p(x) \in F[x]$ is said to be irreducible if its only divisors are its associates and the nonzero constant polynomials. In each part, explain why $[f(x)]$ is a unit in $\mathbb{F}[x]/(p(x))$ and find its inverse.

(a) $[f(x)] = [2x-3] \in \mathbb{Q}[x]/(x^2-2)$.

(b) $[f(x)] = [x^2+x+1] \in \mathbb{Z}_3[x]/(x^2+1)$.

∴

Solution. (a). Since x^2-2 is irreducible in $\mathbb{Q}[x]$, the quotient

$$\mathbb{Q}[x]/(x^2-2)$$

is a field. Thus every nonzero class is a unit. Now $[2x-3] \neq [0]$ in this quotient, since otherwise x^2-2 would divide the linear polynomial $2x-3$, which is impossible. So $[2x-3]$ is a unit. To find its inverse, we solve

$$(2x-3)(ax+b) \equiv 1 \mod (x^2-2).$$

Using $x^2 \equiv 2$, we compute

$$\begin{aligned}(2x-3)(ax+b) &= 2ax^2 + (2b-3a)x - 3b \\ &\equiv 4a + (2b-3a)x - 3b.\end{aligned}$$

So we want

$$(2b-3a)x + (4a-3b) = 1.$$

Thus

$$\begin{aligned}2b-3a &= 0, \\ 4a-3b &= 1.\end{aligned}$$

From the first equation, $2b = 3a$. Over $\mathbb{Q}$ this gives

$$b = \frac{3a}{2}.$$

Substitute into the second:

$$4a - 3\left(\frac{3a}{2}\right) = 1,$$

so

$$\frac{8a-9a}{2} = 1,$$

hence

$$-\frac{a}{2} = 1, \qquad a = -2, \qquad b = -3.$$

Therefore

$$[2x-3]^{-1} = [-2x-3].$$

(b). In $\mathbb{Z}_3[x]/(x^2+1)$, we first reduce

$$x^2+x+1 \equiv 2+x+1 = x$$

since $x^2 \equiv -1 \equiv 2$ modulo x^2+1. So

$$[x^2+x+1] = [x].$$

Since the quotient is a field, any nonzero element is a unit. Also $[x] \neq [0]$, so $[x^2+x+1]$ is a unit. To find its inverse, note that

$$x^2 \equiv 2 \mod (x^2+1),$$

so

$$x \cdot 2x = 2x^2 \equiv 2 \cdot 2 = 4 \equiv 1 \mod 3.$$

Therefore

$$[x]^{-1} = [2x].$$

Hence

$$[x^2+x+1]^{-1} = [2x].$$

□

[12.5.0.5] Problem. Find a fourth-degree polynomial in $\mathbb{Z}_2[x]$ whose roots are the four elements of the field

$$\mathbb{Z}_2[x]/(x^2+x+1).$$

∴

Solution. The field

$$\mathbb{Z}_2[x]/(x^2+x+1)$$

has four elements:

$$[0],\ [1],\ [x],\ [x+1].$$

A polynomial whose roots are exactly these four elements is

$$f(t) = t(t+1)(t+x)(t+x+1).$$

Over a field with 4 elements, every element a satisfies

$$a^4 = a,$$

so the polynomial

$$t^4 - t$$

has all four field elements as roots. Since we are in characteristic 2, this is the same as

$$t^4 + t.$$

Thus one such fourth-degree polynomial is

$$f(t) = t^4 + t.$$

Indeed,

$$f(0) = 0, \qquad f(1) = 1+1 = 0, \qquad f(x) = x^4 + x = 0, \qquad f(x+1) = (x+1)^4 + (x+1) = 0.$$

So the four elements of the field are precisely the roots. □

[12.5.0.6] Problem. (a) Show that $\mathbb{Z}_2[x]/(x^3+x+1)$ is a field.

(b) Show that the field $\mathbb{Z}_2[x]/(x^3+x+1)$ contains all three roots of x^3+x+1.

$\therefore$

Solution. (a). We show that

$$x^3+x+1$$

is irreducible in $\mathbb{Z}_2[x]$. A cubic over a field is reducible if and only if it has a root. So check the two elements of $\mathbb{Z}_2$:

$$f(0) = 0^3+0+1 = 1 \neq 0,$$
$$f(1) = 1^3+1+1 = 1 \neq 0$$

in $\mathbb{Z}_2$. Thus x^3+x+1 has no root in $\mathbb{Z}_2$, so it is irreducible. Therefore

$$\mathbb{Z}_2[x]/(x^3+x+1)$$

is a field.

(b). Let

$$\alpha = [x] \in \mathbb{Z}_2[x]/(x^3+x+1).$$

Then

$$\alpha^3+\alpha+1 = 0$$

in the quotient, since

$$x^3+x+1 \equiv 0 \mod (x^3+x+1).$$

So α is one root. Since we are in characteristic 2, the nonzero elements of this field form a multiplicative group of order 7. Thus every nonzero element satisfies $u^7 = 1$. Now from

$$\alpha^3+\alpha+1 = 0$$

we get

$$\alpha^3 = \alpha+1.$$

Then

$$(\alpha^2)^3+\alpha^2+1 = \alpha^6+\alpha^2+1.$$

Because $\alpha^7 = 1$, we have

$$\alpha^6 = \alpha^{-1}.$$

Also, from $\alpha^3 = \alpha+1$, multiplying by α^{-1} gives

$$\alpha^2 = 1+\alpha^{-1},$$

so

$$\alpha^{-1} = \alpha^2+1.$$

Hence

$$\alpha^6+\alpha^2+1 = (\alpha^2+1)+\alpha^2+1 = 0.$$

So α^2 is also a root. Similarly,

$$\begin{aligned}(\alpha^4)^3+\alpha^4+1 &= \alpha^{12}+\alpha^4+1\\ &= \alpha^5+\alpha^4+1\end{aligned}$$

since $\alpha^7 = 1$. Now

$$\alpha^4 = \alpha(\alpha^3) = \alpha(\alpha+1) = \alpha^2 + \alpha,$$

and

$$\alpha^5 = \alpha(\alpha^4) = \alpha(\alpha^2+\alpha) = \alpha^3 + \alpha^2 = (\alpha+1) + \alpha^2.$$

Thus

$$\alpha^5 + \alpha^4 + 1 = (\alpha^2+\alpha+1) + (\alpha^2+\alpha) + 1 = 0.$$

So α^4 is also a root. Therefore the three roots of x^3+x+1 in this field are

$$[x],\ [x^2],\ [x^4].$$

Hence the field contains all three roots. □

[12.5.0.7] Problem. Show that every polynomial of degree 1, 2, or 4 in $\mathbb{Z}_2[x]$ has a root in

$$\mathbb{Z}_2[x]/(x^4+x+1).$$

∴

Solution. Let

$$E := \mathbb{Z}_2[x]/(x^4+x+1).$$

Since x^4+x+1 is irreducible over $\mathbb{Z}_2$, E is a field with

$$2^4 = 16$$

elements. A finite field of order 16 has multiplicative group of order 15, so every nonzero element $a \in E$ satisfies

$$a^{15} = 1.$$

Thus every nonzero element is a root of

$$t^{15} - 1.$$

Since we are in characteristic 2, this is

$$t^{15} + 1.$$

So all 16 elements of E are roots of

$$t^{16} - t.$$

Now let $f(t) \in \mathbb{Z}_2[t]$ be irreducible of degree 1, 2, or 4. Then the splitting field of f over $\mathbb{Z}_2$ has size 2^d, where $d = \deg f$. Since d is one of $1, 2, 4$, we have

$$d \mid 4.$$

Hence the field with 2^d elements embeds into the field with $2^4 = 16$ elements. Therefore every irreducible polynomial of degree 1, 2, or 4 over $\mathbb{Z}_2$ splits in E, and in particular has a root in E. Since every polynomial of degree 1, 2, or 4 factors into irreducibles whose degrees are among 1, 2, and 4, it follows that every such polynomial has a root in E. Thus every polynomial of degree 1, 2, or 4 in $\mathbb{Z}_2[x]$ has a root in

$$\mathbb{Z}_2[x]/(x^4+x+1).$$

□

12.6 Chapter 7

[12.6.0.1] Problem. Let R be a ring with identity and let I be an ideal in R.

(a). If $1_R \in I$, prove that $I = R$.

(b). If I contains a unit, prove that $I = R$.

$\therefore$

Solution. **(a).** Suppose $1_R \in I$. Let $r \in R$ be arbitrary. Since I is an ideal and $1_R \in I$, we have

$$r1_R = r \in I.$$

Thus every element of R lies in I. Hence $I = R$.

(b). Suppose I contains a unit $u \in R$. Then there exists $u^{-1} \in R$ such that

$$u^{-1}u = 1_R.$$

Since $u \in I$ and I is an ideal, we have

$$u^{-1}u = 1_R \in I.$$

By part **(a)**, it follows that $I = R$. □

[12.6.0.2] Problem. If I is an ideal in a field $\mathbb{F}$, prove that

$$I = (0)_{\mathbb{F}} \quad \text{or} \quad I = \mathbb{F}.$$

$\therefore$

Solution. If $I = (0)_{\mathbb{F}}$, then we are done. Suppose instead that $I \neq (0)_{\mathbb{F}}$. Then there exists some $a \in I$ with $a \neq 0$. Since $\mathbb{F}$ is a field, a is a unit. Therefore, by the previous problem, $I = \mathbb{F}$. Hence every ideal in a field is either $(0)_{\mathbb{F}}$ or $\mathbb{F}$. □

[12.6.0.3] Problem. Let J be an ideal in R. Prove that I is an ideal, where

$$I := \{r \in R : rt = 0_R \text{ for all } t \in J\}.$$

$\therefore$

Solution. First, note that $0_R \in I$, since for every $t \in J$,

$$0_R t = 0_R.$$

Now let $a, b \in I$. Then for every $t \in J$,

$$(a - b)t = at - bt = 0_R - 0_R = 0_R.$$

Thus $a-b\in I$. Now let $r\in R$ and $a\in I$. Then for every $t\in J$,

$$(ra)t = r(at) = r0_R = 0_R.$$

So $ra\in I$. Also, since J is an ideal, we have $rt\in J$ for every $t\in J$. Therefore

$$(ar)t = a(rt) = 0_R$$

for every $t\in J$. So $ar\in I$. Hence I is an ideal of R. □

[12.6.0.4] Problem. Let I and J be ideals in R. Let IJ denote the set of all possible finite sums of elements of the form ab, with $a\in I$ and $b\in J$, that is,

$$IJ := \{a_1b_1+\ldots+a_nb_n : n\geq 1,\ a_k\in I,\ b_k\in J\}.$$

Prove that IJ is an ideal.

∴

Solution. Let

$$x=\sum_{i=1}^{m} a_ib_i\in IJ \quad\text{and}\quad y=\sum_{j=1}^{n} c_jd_j\in IJ.$$

Then

$$x-y=\sum_{i=1}^{m} a_ib_i-\sum_{j=1}^{n} c_jd_j=\sum_{i=1}^{m} a_ib_i+\sum_{j=1}^{n}(-c_j)d_j.$$

Since I is an ideal, $-c_j\in I$ for each j. Thus $x-y$ is again a finite sum of terms of the form ab with $a\in I$ and $b\in J$. So $x-y\in IJ$. Now let $r\in R$. Then

$$rx=r\left(\sum_{i=1}^{m} a_ib_i\right)=\sum_{i=1}^{m}(ra_i)b_i.$$

Since I is an ideal, $ra_i\in I$. Thus $rx\in IJ$. Similarly,

$$xr=\left(\sum_{i=1}^{m} a_ib_i\right)r=\sum_{i=1}^{m} a_i(b_ir).$$

Since J is an ideal, $b_ir\in J$. Thus $xr\in IJ$. Also $0\in IJ$, since if $a\in I$ and $b\in J$, then

$$ab-ab=0$$

is in IJ. Therefore IJ is an ideal of R. □

[12.6.0.5] Problem. Prove that every ideal in $\mathbb{Z}$ is principal.

∴

Solution. Let I be an ideal of $\mathbb{Z}$. If $I=\{0\}$, then

$$I=(0),$$

so I is principal. Suppose $I\neq\{0\}$. Since I contains a nonzero integer, it contains a positive integer. Let $c\in I$ be the smallest positive integer in I. We claim that

$$I=(c).$$

First, since $c \in I$ and I is an ideal, every multiple of c lies in I. Thus

$$(c) \subseteq I.$$

Now let $a \in I$. By the division algorithm, there exist integers q and r such that

$$a = qc + r \quad \text{with} \quad 0 \leq r < c.$$

Since $c \in I$, we have $qc \in I$. Also $a \in I$. Thus

$$r = a - qc \in I.$$

But c was chosen to be the smallest positive integer in I. Since $0 \leq r < c$, it follows that $r = 0$. Hence

$$a = qc \in (c).$$

So $I \subseteq (c)$. Therefore

$$I = (c),$$

and every ideal in $\mathbb{Z}$ is principal. □

[12.6.0.6] Problem. Let $\mathbb{F}$ be a field. Prove that every ideal in $\mathbb{F}[x]$ is principal.

∴

Solution. Let I be an ideal in $\mathbb{F}[x]$. If $I = \{0\}$, then

$$I = (0),$$

so I is principal. Suppose $I \neq \{0\}$. Choose a nonzero polynomial $b(x) \in I$ of smallest degree. We claim that

$$I = (b(x)).$$

First, since $b(x) \in I$ and I is an ideal, every multiple of $b(x)$ lies in I. Thus

$$(b(x)) \subseteq I.$$

Now let $a(x) \in I$. By the division algorithm in $\mathbb{F}[x]$, there exist polynomials $q(x), r(x) \in \mathbb{F}[x]$ such that

$$a(x) = q(x)b(x) + r(x),$$

where either $r(x) = 0$ or

$$\deg r(x) < \deg b(x).$$

Since $b(x) \in I$, we have $q(x)b(x) \in I$. Also $a(x) \in I$. Therefore

$$r(x) = a(x) - q(x)b(x) \in I.$$

By the minimality of the degree of $b(x)$, we must have $r(x) = 0$. Hence

$$a(x) = q(x)b(x) \in (b(x)).$$

So $I \subseteq (b(x))$. Therefore

$$I = (b(x)),$$

and every ideal in $\mathbb{F}[x]$ is principal. □

[12.6.0.7] Problem. Show that every homomorphic image of a field $\mathbb{F}$ is isomorphic either to $\mathbb{F}$ itself or to the zero ring.

$\therefore$

Solution. Let $f : \mathbb{F} \to S$ be a ring homomorphism. Let

$$K = \ker f.$$

Since $\mathbb{F}$ is a field, its only ideals are (0) and $\mathbb{F}$. Therefore

$$K = (0) \quad \text{or} \quad K = \mathbb{F}.$$

If $K = (0)$, then by the First Isomorphism Theorem,

$$\mathbb{F}/(0) \cong \operatorname{Im}(f),$$

so

$$\operatorname{Im}(f) \cong \mathbb{F}.$$

If $K = \mathbb{F}$, then f is the zero homomorphism, so its image is the zero ring. Hence every homomorphic image of a field is isomorphic either to the field itself or to the zero ring. □

[12.6.0.8] Problem. Use the First Isomorphism Theorem to show that

$$\mathbb{Z}_{20}/(5) \cong \mathbb{Z}_5.$$

$\therefore$

Solution. Define

$$f : \mathbb{Z}_{20} \to \mathbb{Z}_5$$

by

$$f([a]_{20}) = [a]_5.$$

First we check that f is well-defined. Suppose

$$[a]_{20} = [b]_{20}.$$

Then

$$a \equiv b \mod 20,$$

so

$$20 \mid (a - b).$$

Hence

$$5 \mid (a - b),$$

which means

$$[a]_5 = [b]_5.$$

Therefore f is well-defined. Now we check that f is a ring homomorphism. For addition,

$$\begin{aligned} f([a]_{20} + [b]_{20}) &= f([a + b]_{20}) \\ &= [a + b]_5 \\ &= [a]_5 + [b]_5 \end{aligned}$$

$$= f([a]_{20}) + f([b]_{20}).$$

For multiplication,

$$\begin{aligned} f([a]_{20}[b]_{20}) &= f([ab]_{20}) \\ &= [ab]_5 \\ &= [a]_5[b]_5 \\ &= f([a]_{20})f([b]_{20}). \end{aligned}$$

The map is surjective, since every class $[a]_5 \in \mathbb{Z}_5$ is the image of $[a]_{20}$. Now compute the kernel. We have

$$f([a]_{20}) = [0]_5$$

if and only if

$$[a]_5 = [0]_5,$$

which holds if and only if $5 \mid a$. Thus

$$\ker f = (5).$$

By the First Isomorphism Theorem,

$$\mathbb{Z}_{20}/(5) \cong \mathrm{Im}(f) = \mathbb{Z}_5.$$

□

[12.6.0.9] Problem. Let I and J be ideals in a ring R. Then $I \cap J$ is an ideal in I, and J is an ideal in $I + J$. Prove that

$$\frac{I}{I \cap J} \cong \frac{I+J}{J}.$$

Solution. Define

$$f : I \to \frac{I+J}{J}$$

by

$$f(a) = a + J.$$

First we check that f is a ring homomorphism. If $a, b \in I$, then

$$\begin{aligned} f(a+b) &= (a+b) + J \\ &= (a+J) + (b+J) \\ &= f(a) + f(b). \end{aligned}$$

Also,

$$\begin{aligned} f(ab) &= ab + J \\ &= (a+J)(b+J) \\ &= f(a)f(b). \end{aligned}$$

Now we show f is surjective. An arbitrary element of $(I+J)/J$ has the form

$$(a+j) + J$$

with $a \in I$ and $j \in J$. But

$$(a+j)+J = a+J = f(a).$$

So f is surjective. Now compute the kernel. We have

$$f(a) = J$$

if and only if

$$a+J = J,$$

which happens if and only if $a \in J$. Since also $a \in I$, this means

$$a \in I \cap J.$$

Thus

$$\ker f = I \cap J.$$

By the First Isomorphism Theorem,

$$\frac{I}{I \cap J} \cong \frac{I+J}{J}.$$

□

12.7 Chapter 8

[12.7.0.1] Problem. Find the minimal polynomial of the given element over $\mathbb{Q}$.

(a). $\sqrt{1+\sqrt{5}}$.

(b). $\sqrt{3}i+\sqrt{2}$.

∴

Solution. (a). Let

$$\alpha := \sqrt{1+\sqrt{5}}.$$

Then

$$\alpha^2 = 1+\sqrt{5},$$
$$\alpha^2 - 1 = \sqrt{5}.$$

Squaring again gives

$$(\alpha^2-1)^2 = 5,$$
$$\alpha^4 - 2\alpha^2 + 1 = 5,$$
$$\alpha^4 - 2\alpha^2 - 4 = 0.$$

So α is a root of

$$f(x) = x^4 - 2x^2 - 4.$$

Now we show that $f(x)$ is irreducible over $\mathbb{Q}$. Suppose

$$x^4 - 2x^2 - 4 = (x^2 + ax + b)(x^2 - ax + d)$$

for some $a, b, d \in \mathbb{Q}$. Expanding gives

$$x^4 + (b + d - a^2)x^2 + a(d - b)x + bd.$$

Comparing coefficients, we get

$$\begin{aligned} bd &= -4, \\ b + d - a^2 &= -2, \\ a(d - b) &= 0. \end{aligned}$$

If $a = 0$, then

$$x^4 - 2x^2 - 4 = (x^2 + b)(x^2 + d),$$

so

$$b + d = -2 \quad \text{and} \quad bd = -4.$$

Thus b and d would be roots of

$$t^2 + 2t - 4 = 0,$$

whose discriminant is

$$2^2 - 4(1)(-4) = 20,$$

not a square in $\mathbb{Q}$. So this is impossible. If $d = b$, then

$$bd = b^2 = -4,$$

which is impossible in $\mathbb{Q}$. Thus $f(x)$ is irreducible over $\mathbb{Q}$. Hence the minimal polynomial of $\sqrt{1 + \sqrt{5}}$ over $\mathbb{Q}$ is

$$x^4 - 2x^2 - 4.$$

(b). Let

$$\beta := \sqrt{3}i + \sqrt{2}.$$

Then

$$\begin{aligned} \beta - \sqrt{2} &= \sqrt{3}i, \\ (\beta - \sqrt{2})^2 &= -3. \end{aligned}$$

So

$$\begin{aligned} \beta^2 - 2\sqrt{2}\beta + 2 &= -3, \\ \beta^2 - 2\sqrt{2}\beta + 5 &= 0, \\ \beta^2 + 5 &= 2\sqrt{2}\beta. \end{aligned}$$

Squaring again gives

$$\begin{aligned} (\beta^2 + 5)^2 &= 8\beta^2, \\ \beta^4 + 10\beta^2 + 25 &= 8\beta^2, \\ \beta^4 + 2\beta^2 + 25 &= 0. \end{aligned}$$

So β is a root of

$$g(x) = x^4 + 2x^2 + 25.$$

Now we show that $g(x)$ is irreducible over $\mathbb{Q}$. Suppose

$$x^4 + 2x^2 + 25 = (x^2 + ax + b)(x^2 - ax + d)$$

for some $a, b, d \in \mathbb{Q}$. Expanding gives

$$x^4 + (b + d - a^2)x^2 + a(d - b)x + bd.$$

Comparing coefficients, we get

$$bd = 25,$$
$$b + d - a^2 = 2,$$
$$a(d - b) = 0.$$

If $a = 0$, then

$$x^4 + 2x^2 + 25 = (x^2 + b)(x^2 + d),$$

so

$$b + d = 2 \quad \text{and} \quad bd = 25.$$

Thus b and d would be roots of

$$t^2 - 2t + 25 = 0,$$

whose discriminant is

$$(-2)^2 - 4(1)(25) = -96,$$

not a square in $\mathbb{Q}$. So this is impossible. If $d = b$, then

$$b^2 = 25,$$

so $b = \pm 5$. If $b = 5$, then

$$2b - a^2 = 2$$

gives

$$10 - a^2 = 2,$$

so

$$a^2 = 8,$$

which is impossible in $\mathbb{Q}$. If $b = -5$, then

$$2b - a^2 = 2$$

gives

$$-10 - a^2 = 2,$$

so

$$a^2 = -12,$$

also impossible in $\mathbb{Q}$. Thus $g(x)$ is irreducible over $\mathbb{Q}$. Hence the minimal polynomial of $\sqrt{3}i + \sqrt{2}$ over $\mathbb{Q}$ is

$$x^4 + 2x^2 + 25.$$

□